Upgrading Avaya Breeze® platform

Release 3.9
Issue 5
October 2026

© 2013-2026 Avaya LLC.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

"**Hosted Service**" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE

PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Purpose 8
Required permissions 8
Change history 8

Chapter 2: Upgrade preparation guidelines 10
Upgrade compatibility and system interactions 10
Avaya Breeze® platform compatibility 10
Upgrade licensing 11
VMware ESXi upgrades and maintenance 11
Avaya Aura® Media Server selection algorithm 11

Chapter 3: Upgrading an Avaya Breeze® platform 13
Supported Avaya Breeze® platform upgrade paths 13
GDPR compliance 14
VMware ESXi upgrades and maintenance 15

Chapter 4: Method 1: Upgrading using OVA reinstallation 16
Checklist for upgrade method 1 - Upgrading using OVA reinstallation 16
Obtaining the configuration information 21
Customer configuration information for OVA upgrades 22
Administering Avaya Aura® Media Server for REST 26
Assigning Avaya Aura® Media Server for use with Avaya Breeze® platform 27
Backing up the cluster database 27
Installing the clusterDBMigration service 28
Backing up the cluster database 28
Disabling the secure grid 29
Downloading software from PLDS 29
Verifying the enrollment password status 30
Verifying the signature algorithm of their existing LDAP/LDAPS server certificate 30
Setting the cluster to Deny New Service status 31
Verifying there is no server activity 31
Uninstalling and deleting snap-ins 32
Removing the existing servers from the cluster 32
Shutting down the existing servers 33
Deploying the replacement upgrade release servers 34
Deploying Avaya Breeze® platform OVA with VMware vSphere Client connected to vCenter 34
Deploying Avaya Breeze® platform OVA with VMware vSphere Web Client 35

Deploying Avaya Breeze® platform OVA with VMware vSphere Client connected to ESXi host 37
Deploying Avaya Breeze® platform OVA with Solution Deployment Manager 40
Configure the new server automatic startup settings 42
Configuring virtual machine automatic startup settings using vSphere desktop client 42
Configuring virtual machine automatic startup settings using vSphere Web Client 43
Changing the customer password on first login 44
Creating multiple privileged user accounts 44
Installing the upgrade patch if required 44
Setting preferred snap-in version 45
Removing the clusterDBMigrationService 46
Adding the new servers to the cluster 47
Editing the cluster attributes 47
Enabling the secure grid 47
Verifying replication status 48
Running maintenance tests 48
Verifying the status of the new servers 48
Installing new and upgraded snap-ins 49
Restoring the cluster database 50
Rebooting a cluster 50
Adding a trusted certificate to all Avaya Breeze® platform servers in a cluster 50
Setting the cluster back to Accepting New Service status 51
Verifying the Avaya Breeze® platform entity link connection 51

Chapter 5: Method 2: Upgrading using simultaneous cluster upgrade 53
Checklist for upgrade method 2 - Simultaneous cluster upgrade 53
Customer configuration information for ISO upgrades 58
Downloading software from PLDS 58
Disabling the secure grid 59
Verifying Enrollment Password status 59
Denying new service 60
Updating the Subject Alternative Name on the Manage Identity Certificate 60
Verify activity 61
Upgrading the Avaya Breeze® platform server 61
Upgrades using Solution Deployment Manager 61
Checklist for upgrading Avaya Breeze® platform using Solution Deployment Manager 62
Installing the Solution Deployment Manager client 63
Installing the OVA file into the software library 65

Downloading the version_edp.xml file 65
Re-establishing a trust connection 65
Refreshing the host status 66
Refreshing elements 66
Analyzing software 67
Performing the pre-upgrade check 67
Upgrading Avaya Breeze® platform using Solution Deployment Manager 68
Committing the upgrade of Avaya Breeze® platform 69
Verifying replication status 70
Running maintenance tests 70
Verifying server status 71
Accepting new service 71
Verifying the Entity Link connection 71
Installing new snap-ins 72
Setting preferred snap-in version 72

Chapter 6: Method 3: Upgrading using rolling cluster upgrade 74
Checklist for upgrade method 3 - Rolling cluster upgrade 74
Customer configuration information for ISO upgrades 78
Server upgrade sequence 78
Viewing and changing server cluster database status 79
Downloading software from PLDS 79
Disabling the secure grid 80
Verifying Enrollment Password status 80
Denying new service 81
Updating the Subject Alternative Name on the Manage Identity Certificate 81
Verify activity 82
Upgrading the Avaya Breeze® platform server 82
Upgrades using Solution Deployment Manager 82
Checklist for upgrading Avaya Breeze® platform using Solution Deployment Manager 62
Installing the Solution Deployment Manager client 84
Installing the OVA file into the software library 86
Downloading the version_edp.xml file 86
Re-establishing a trust connection 86
Refreshing the host status 87
Refreshing elements 87
Analyzing software 88
Performing the pre-upgrade check 88
Upgrading Avaya Breeze® platform using Solution Deployment Manager 68

Committing the upgrade of Avaya Breeze® platform 90
Verifying replication status 91
Running maintenance tests 91
Verifying server status 92
Accepting new service 92
Verifying the Entity Link connection 92
Installing new snap-ins 93
Setting preferred snap-in version 93

Chapter 7: Enhanced Access Security Gateway 95
Enabling and disabling EASG 95
Viewing the EASG certificate information 95
EASG site certificate 96
Managing site certificates 96

Chapter 8: Patching 97
Determining patching sequence 97
Patching the Avaya Breeze® platform 97
Patch command options 98

Appendix A: VMware snapshots 99
VMware snapshots 99

Appendix B: Removing obsolete Avaya Aura Media Server configuration 101
Removing obsolete Avaya Aura® Media Server configuration 101

Appendix C: Documentation for Collaboration Environment 103
Additional information 103

Chapter 1: Purpose

This document provides procedures for upgrading Avaya Breeze® platform. It includes checklists, upgrade procedures, and verification procedures for each supported upgrade path.

Required permissions

To upgrade Avaya Breeze® platform, you must have permissions to:

- Log in to a craft or customer account.

  When you log in to your customer account for the first time, you must change the password. For information about changing your customer account password, see *Deploying Avaya Breeze® platform*.
- Administer the Avaya Breeze® platform element on System Manager.

Change history

Issue	Date	Summary of changes
1	December 2023	• Updates for Avaya Breeze® platform R3.9.
2	January 2024	• Add maximum active SIP sessions value for profile 5. See "Customer configuration information for OVA upgrades" on page 22.
3	February 2024	• Corrections to web links to other Avaya Breeze® platform documents.
4	November 2025	Updated the following sections for Release 3.9.0.3: • Checklist for upgrade method 1 - Upgrading using OVA reinstallation. • Supported upgrade paths.

Table continues

Issue	Date	Summary of changes
5	October 2026	Updated the following sections for Release 3.9.0.4: • Checklist for upgrade method 1 - Upgrading using OVA reinstallation • Checklist for upgrade method 2 - Simultaneous cluster upgrade October 2026 Upgrading Avaya Breeze® platform Comments on • Checklist for upgrade method 3 - Rolling cluster upgrade Added the following new sections: • Verifying the signature algorithm of their existing LDAP/LDAPS server certificate • Updating the Subject Alternative Name on the Manage Identity Certificate

Chapter 2: Upgrade preparation guidelines

Before upgrading Avaya Breeze® platform, you must first upgrade Avaya Aura® Media Server, System Manager, and other Avaya Aura® components used.

- For information about upgrading Avaya Aura® Media Server, see *Deploying and Updating Avaya Aura® Media Server Appliance*.
- For more information about System Manager upgrades, see *Upgrading Avaya Aura® System Manager*.

Upgrade compatibility and system interactions

Avaya Breeze® platform can interwork with the latest System Manager Release 10.1.2.x (Avaya Breeze® platform 3.9.0.0 only), 10.1.3.x, 10.2, and 10.3. For more information, see "Avaya Breeze platform compatibility" on page 10.

- For snap-ins that process calls, Avaya Breeze® platform requires Session Manager Release 6.3.8 or above.
- For snap-ins that use the Avaya Aura® Media Server, Avaya Breeze® platform requires Avaya Aura® Media Server Release 8.0.2 or above.

The Avaya Breeze® platform supports snap-ins built with SDK Release 3.0 and above. Contact your snap-in vendor for your specific combination or for any other concerns related to your snap-in. For more information about known issues that might impact your snap-in, refer to the *Avaya Breeze® platform Release Notes*.

For more information about interoperability, see:

- *Avaya Breeze® platform Overview and Specification*
- https://support.avaya.com/CompatibilityMatrix/Index.aspx

Avaya Breeze® platform compatibility

You can deploy Avaya Breeze® platform with the latest System Manager R10.3.x.

For information about Avaya product compatibility, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml.

System Manager version	Supported Element Manager/JDK
10.2.1.4 and earlier	JDK 8-based Element Manager

Table continues

System Manager version	Supported Element Manager/JDK
10.3 and later	JDK 11-based Element Manager

Important:

- You must verify the System Manager version and corresponding EM/JDK compatibility before starting an Element Manager installation.
- Installing a JDK 11-based EM on an unsupported System Manager version may leave the System Manager system in an unusable state, for example, the System Manager URL may become inaccessible.
- Installing a JDK 8-based Element Manager later does not provide a recovery path once an unsupported JDK 11-based Element Manager installation has occurred.
- Verify the System Manager version and Element Manager/JDK compatibility before installation and take the System Manager snapshot or backup before installing Element Manager.

Upgrade licensing

Upgrading Avaya Breeze® platform to Release 3.9 does not require a new Avaya Breeze® platform license file. However, if you need to perform an OVA upgrade for System Manager, you must install a new Avaya Breeze® platform license during that upgrade, unless you use the Solution Deployment Manager (SDM) client for the System Manager upgrade. For more information about System Manager upgrades, see *Upgrading Avaya Aura® System Manager*.

Avaya Breeze® platform uses the Avaya Product Licensing and Delivery System (PLDS) to manage license entitlement and generate license files. License files are downloadable from PLDS and installed on System Manager WebLM. In a network with multiple Avaya Breeze® platform servers and clusters, you can use a single license file installed on System Manager WebLM to license all the Avaya Breeze® platform servers.

VMware ESXi upgrades and maintenance

For upgrade and maintenance actions required for the ESXi platforms hosting Avaya Breeze® platform servers, refer to the *Maintaining and Troubleshooting Avaya Breeze® platform* manual.

Avaya Aura® Media Server selection algorithm

Avaya Breeze® platform supports a rich algorithm for selecting which Avaya Aura® Media Server to use for each call. The algorithm uses the locations defined in the System Manager routing. You can assign locations as follows:

- You can assign locations explicitly to a SIP entity such as the Avaya Breeze® platform.
- You can specify IP address patterns for locations. Avaya Breeze® platform uses the address patterns to match the IP address of endpoints and SIP entities to locations.

The selection algorithm can also include optional rules which Avaya Breeze® platform uses in the following order:

1. Check the location of the caller

   If the caller's SIP endpoint or SIP entity, such as a trunk gateway, matches an assigned location, Avaya Breeze® platform attempts to assign the Avaya Aura® Media Server that is in the same location.
2. Check the location of the Avaya Breeze® platform server

   If the Avaya Breeze® platform server handling a call has an assigned location, Avaya Breeze® platform attempts to assign the Avaya Aura® Media Server in the same location.
3. Select a lightly-loaded Avaya Aura® Media Server from any location.

If none of these rules match, the call fails. New clusters have all the rules enabled by default. To preserve backward compatible behavior, any existing clusters do not have the first rule enabled by default. If required, you can enable the rule after upgrading.

You can select which rules on the Cluster Editor screen displayed when you click **New** or **Edit** on the Cluster Administration page. For more information, see "Cluster Editor field descriptions" in *Administering Avaya Breeze® platform*.

Chapter 3: Upgrading an Avaya Breeze® platform

You can use a number of different upgrade methods. The supported method depends on the Avaya Breeze® platform release and whether you want can perform the upgrade during a maintenance window.

Method	Description
1.	**OVA Reinstallation** This method of upgrading requires the reinstallation of the Avaya Breeze® platform OVA on each server in the cluster after removing all nodes from the cluster. Cluster database and data grid data are not preserved. • This upgrade method is service impacting and should only be performed during a maintenance window.
2.	**Simultaneous Cluster Upgrade** You can use this method to simultaneously upgrade all nodes within a cluster within five minutes of each other. • This upgrade method is service impacting and should only be performed during a maintenance window. • This method is only supported with Avaya Breeze® platform R3.3 and higher. For more information, see: "Supported Avaya Breeze platform upgrade paths" on page 13 • Optionally, this method can use System Manager Solution Deployment Manager (SDM).
3.	**Rolling Cluster Upgrade** You can use this method to perform rolling upgrade of each node within a cluster in turn. This upgrade method is not service impacting. • This method is only supported with Avaya Breeze® platform R3.3 and higher. For more information, see: "Supported Avaya Breeze platform upgrade paths" on page 13. • Optionally, this method can use System Manager Solution Deployment Manager (SDM).

Supported Avaya Breeze® platform upgrade paths

Select an upgrade method from the following table.

Release	Upgrade method
3.0.x to 3.9.x	• "Method 1: Upgrading using OVA reinstallation" on page 16 **Note:** • Do not add Release 3.8.x or earlier nodes to an upgraded Release 3.9.x cluster.
3.1.x to 3.9.x	
3.2.x to 3.9.x	
3.3.x to 3.9.x	
3.4.x to 3.9.x	
3.5.x to 3.9.x	
3.6.x to 3.9.x	
3.7.x to 3.9.x	
3.8.x to 3.9.x	
3.9.0.0 to 3.9.0.x	
3.9.0.2 to 3.9.0.x	Supports Method 1 or Method 2 or Method 3
3.9.0.3 to 3.9.0.x	"Method 1: Upgrading using OVA reinstallation" on page 16 "Method 2: Upgrading using simultaneous cluster upgrade" on page 53 "Method 3: Upgrading using rolling cluster upgrade" on page 74

GDPR compliance

All the data to and from Avaya Breeze® platform nodes is encrypted using TLS in transit.

You can choose to encrypt your Avaya Breeze® platform virtual machine (VM) for General Data Protection Regulation (GDPR) compliance using VMware provided encryption. You can encrypt an existing VM or encrypt a new one you are deploying. The procedure requires a Key Management Server (KMS). Follow the vCenter virtual machine encryption instructions in your VMware documentation.

Encrypting your VM will reduce the capacity of your server. How much depends on the resources used by the installed snap-ins. Snap-ins that use the system storage (including the local cluster database) will notice a greater capacity decrease.

For additional information about GDPR compliance, see *Avaya Breeze® platform Overview and Specification*.

VMware ESXi upgrades and maintenance

For upgrade and maintenance actions required for the ESXi platforms hosting Avaya Breeze® platform servers, refer to the *Maintaining and Troubleshooting Avaya Breeze® platform* manual.

Chapter 4: Method 1: Upgrading using OVA reinstallation

If upgrading pre-R3.9 servers,use this method for upgrading to Avaya Breeze® platform R3.9. Do not use any other upgrade methods.

Note:

If upgrading from 3.9.0.0 to higher, use the procedure and skip the clusterDB migration.

- For upgrades to R3.9, use of the clusterDBMigrationService-3.9.0.0 service allows restoration of the pre-R3.9 cluster database following the upgrade.
- The data grid data is not preserved.
- This upgrade method is service impacting and should only be performed during a maintenance window.
- After upgrading and using Avaya Aura® Media Server, you must configure the new REST based configuration.
    - If not using Avaya Engagement Assistant Snap-in, remove the existing Avaya Aura® Media Server SIP version of the configuration.
    - If using Avaya Engagement Assistant Snap-in, leave the existing Avaya Aura® Media Server SIP version configuration.

Checklist for upgrade method 1 - Upgrading using OVA reinstallation

Upgrades using an OVA file are service-impacting. Perform the upgrades during a maintenance window.

#	Action	Link/Notes	✔
1.	Check the prerequisites and post-upgrade tasks for snap-ins before proceeding with the upgrade.	Refer to the snap-in documentation.	

Table continues

#	Action	Link/Notes	✔
2.	Obtain information for the existing Avaya Breeze® platform servers.	• "Obtaining the configuration information" on page 21 • "Customer configuration information for OVA upgrades" on page 22	
3.	Before upgrading Avaya Breeze® platform, upgrade the following in this order as needed: 1. System Manager 2. Session Manager	See *Upgrading Avaya Aura® System Manager* and *Upgrading Avaya Aura® Session Manager*. If only upgrading the Avaya Breeze® platform Element Manager, use the **`upgradeSolution`** script. Refer to *Deploying Avaya Breeze® platform*.	
4.	Upgrade Avaya Aura® Media Server.	See *Deploying and Updating Avaya Aura® Media Server Appliance*.	
5.	Enroll Avaya Aura® Media Server on System Manager.	See "System Manager enrollment" section in *Implementing and Administering Avaya Aura® Media Server*.	
6.	If you are using Avaya Aura® Media Server but not Engagement Assistant, remove the obsolete Avaya Aura® Media Server configuration.	See "Removing obsolete Avaya Aura Media Server configuration" on page 101.	
7.	Administer Avaya Aura® Media Server for REST.	See "Administering Avaya Aura Media Server for REST" on page 26	
8.	Assign Avaya Aura® Media Server for use with Avaya Breeze® platform.	See "Assigning Avaya Aura Media Server for use with Avaya Breeze platform" on page 27	
9	If you are using cluster database and upgrading from pre-R 3.9, take a databse backup.	This is a precaution in case it becomes necessary to roll back to the pre-R3.9 release. See Backing up a cluster database.	

Table continues

#	Action	Link/Notes	✔
10.	If using a cluster database on Avaya Breeze® platform 3.8.x or earlier, load and install the clusterDBMigrationService-3.9.0.0 service. If you are using cluster database on Avaya Breeze® platform 3.9.x or later skip this step. This service is pre-loaded on the Avaya Breeze® platform 3.9.x EM and versioned as a 3.9.x snap-in; however, the snap-in is compatible and intended to be installed on 3.8.1.1. and earlier Avaya Breeze® platform clusters.	See "Installing the clusterDBMigration service" on page 28.	
11.	Download the Avaya Breeze® platform OVA and patch file (if required) from PLDS.	See "Downloading software from PLDS" on page 29.	
12.	Verify that the enrollment password has not expired.	See "Verifying the enrollment password status" on page 30.	
13.	Verify the signature algorithm of any existing LDAP/LDAPS server certificate.	"Verifying the signature algorithm of their existing LDAP/LDAPS server certificate" on page 30	
14.	Change the state of the cluster you are upgrading to **Deny New Service**.	See "Setting the cluster to Deny New Service status" on page 31.	
15.	For pre-R 3.9.0 If the cluster database is enabled, take a backup which will use the clusterDBMigrationService-3.9.0.0 to update the schema for use with 3.9. If you are using 3.9.0 or higher, take the cluster database backup.	See Backing up a cluster database.	
16.	Check the cluster **Activity** field is 0.	See "Verifying there is no server activity" on page 31.	

Table continues

#	Action	Link/Notes	✔
17.	Uninstall the Analytics Collector Snap-in and Engagement Call Control from the cluster.	See "Uninstalling and deleting snap-ins" on page 32	
18.	Remove any other solution snap-ins if required.	Refer to the snap-in documentation. for guidance on snap-ins that must be removed before upgrading.	
19.	Remove all Avaya Breeze® platform servers from the cluster.	See "Removing the existing servers from the cluster" on page 32	
20.	Shut down all the existing servers in the cluster.	See "Shutting down the existing servers" on page 33.	
21.	Deploy new servers using the new release OVA. Breeze 3.9 requires an additional 2GB of RAM and 5GB of disk per deployment profile. The presented profiles reflect this information.	See "Deploying the replacement upgrade release servers" on page 34.	
22.	Disable the secure grid if enabled	See "Disabling the secure grid" on page 29.	
23.	Upgrade the mandatory snap-ins and connector snap-ins, including the Authorization service if required by your solution.	See your snap-in documentation.	
24.	You must configure all customized resources (cpu/memorydisk sizes) again after you install the Avaya Breeze® platform OVA.	If you use the cluster database, ensure that the disk size configuration is appropriate for the snap-in that uses the database.	
25.	Configure the virtual machine automatic startup settings.	See "Configure the new server automatic startup settings" on page 42.	
26.	Change the customer password on first login.	See ."Changing the customer password on first login" on page 44.	
27.	Create multiple privileged user accounts.	See "Creating multiple privileged user accounts" on page 44.	

Table continues

#	Action	Link/Notes	✔
28.	Install the patch file if required.	See "Installing the upgrade patch if required" on page 44.	
29.	Set the preferred version for each snap-in.	See "Setting preferred snap-in version" on page 45.	
30.	Remove the clusterDBMigrationService-3.9.0.0 service.	See "Removing the clusterDBMigrationService" on page 46.	
31.	Edit the cluster and clear the **Pre-3.8.1 Cluster** cluster attribute if set.	See "Editing the cluster attributes" on page 47.	
32.	Add the new servers to the cluster.	See "Adding the new servers to the cluster" on page 47	
33.	Select **Enable Database Auto Switchover** (**Elements › Avaya Breeze® › Cluster Administration**).	This is only required for multi-node clusters with a cluster database.	
34.	Optional: Enable Secure Grid.	See "Enabling the secure grid" on page 47.	
35.	Verify data replication between System Manager and Avaya Breeze® platform.	See "Verifying replication status" on page 48.	
36.	Run Avaya Breeze® platform maintenance tests for each server in the cluster.	See "Running maintenance tests" on page 48. Resolve errors before proceeding.	
37.	Verify the status of each of the new servers.	See "Verifying the status of the new servers" on page 48.	
38.	Install new snap-ins.	See "Installing new and upgraded snap-ins" on page 49.	
39.	If using a cluster database, restore the database.	See "Restoring the cluster database" on page 50.	
40.	For a multi-node cluster, reboot the cluster.	See "Rebooting a cluster" on page 50.	

Table continues

#	Action	Link/Notes	✔
41.	Add trust certificates.	For information, see "Adding a trusted certificate to all Avaya Breeze platform servers in a cluster" on page 50.	
42.	Set the cluster state back to **Accept New Service**.	See "Setting the cluster back to Accepting New Service status" on page 51.	
43.	Verify the Avaya Breeze® platform SIP entity link with Session Manager.	See "Verifying the Avaya Breeze platform entity link connection" on page 51.	
44.	Test Avaya Breeze® platform snap-ins to verify that they are functioning correctly.	–	
45.	After a successful upgrade, delete the previous Avaya Breeze® platform server images.	–	
46.	Configure System Manager to receive Avaya Breeze® platform alarms.	See the SNMP support information in *Maintaining and Troubleshooting Avaya Breeze® platform*.	

Obtaining the configuration information

About this task

Use this procedure to obtain the system information. You will need this for configuring the new Avaya Breeze® platform servers installed during the upgrade as replacements for the existing old servers. Record this information in "Customer configuration information for OVA upgrades" on page 22.

Procedure

1. Log in to Avaya Breeze® platform CLI interface.
2. Run the `ceconfig` command.

   The `ceconfig` command displays the following information:

   - IP address
   - Short hostname
   - Network domain
   - Netmask
   - Default gateway
   - DNS servers
   - Time zone
   - NTP servers

- Primary System Manager IP address
- Primary System Manager FQDN

3. Record this information.
4. Record the HTTP Proxy settings for the server on vCenter.

   Alternatively, you can run the `CEnetSetup` command to obtain the HTTP Proxy settings.

Customer configuration information for OVA upgrades

You require the following information to upgrade Avaya Breeze® platform with an OVA. Ensure that you have this information before you begin the upgrade.

Network Settings

Field	Information to enter	Notes
IP Address	Enter the server's IPv4 address.	Management IP address to be assigned to Avaya Breeze® platform.
Short Hostname	Enter the server's host name.	The hostname must match the one for the server that is being upgraded.
Network Domain	Enter the network domain or type `none`.	The network domain must match the one for the server that is being upgraded.
Netmask	Enter IPv4 netmask information.	—
Default gateway	Enter the IP address for the IPv4 gateway.	Default IPv4 gateway for Avaya Breeze® platform management network interface.
IPv6 Address	(Optional) Enter the IPv6 address for the management interface.	Set the **IPv6 Address**, **IPv6 Prefix**, and **IPv6 Gateway** to prepopulate the IPv6 address on the management (eth0) interface. The IPV4 fields are required even if administering IPv6 addresses.
IPv6 Prefix	(Optional) Enter the IPv6 prefix for the management interface.	The IPv4 **Netmask** is still required.
IPv6 Gateway	(Optional) Enter the IPv6 gateway for the management interface.	The IPv6 gateway address that can route the IPv6 addresses. The **Default gateway** IPv4 address is still required.

Table continues

Field	Information to enter	Notes
DNS servers	Enter the primary, secondary, and tertiary DNS server IP address.	You can have up to three DNS servers. Avaya recommends provisioning at least two DNS servers that are resilient in case of power or network failure.
Cluster IP address	Enter a unique IP address.	This value is required after deployment.

Proxy settings

Field	Information to enter
HTTP Proxy Server	Enter the IP address or FQDN of the HTTP proxy server.
HTTP Proxy Port	Enter the HTTP proxy port.
HTTPS Proxy Server	Enter the IP address or FQDN of the HTTPS proxy server.
HTTPS Proxy Port	Enter the HTTPS proxy port.
HTTP Proxy exclusion list	Enter the HTTPS proxy servers with a delimiter of “|”. For example: `*ca.avaya.com|*.us.avaya.com|135.9.95.*` By default, the customer domain will be added to the proxy exclusion list. The proxy exclusion list can be added with the **`CEnetSetup`** command or using the OVA properties during deployment. If the destination for the HTTP request matches any address in the exclusion list, the HTTP request will be sent directly to the destination instead of the proxy.

System Time Settings

Field	Information to enter	Notes
Timezone	Select the timezone from this field.	This configuration is mandatory for Avaya Breeze® platform to function. The timezone configured on Avaya Breeze® platform must match the timezone on System Manager.

Table continues

Field	Information to enter	Notes
NTP Servers	Enter the IP address or FQDN of the primary NTP server.	You can have up to three NTP servers. Enter a value in this field only when the VMware host does not synchronize on its own.

User access

Field	Information to enter	Notes
Enhanced Access Security Gateway (EASG)	Enter one of the following: • `1` to enable EASG. • `2` to disable EASG. Avaya recommends that you enable EASG.	By disabling EASG, you are denying Avaya access to the system. This setting is not recommended as it can impact Avaya's ability to provide support for the product. Unless the customer can manage the product, Avaya Services Logins should not be disabled.

Customer Login Settings

Field	Information to enter	Notes
Login Name	Enter the login ID to use for the customer account (cust).	Login ID and password for customer account you will create during OVA deployment.
Password	Enter the customer account password.	This password will change after first customer login.
Customer Root Password	Enter the customer account root password.	Optional. Available only with SDM upgrades.
Additional user accounts		Record information here that is required to recreate additional user accounts. **Note:** Only one customer account can be created during OVA deployment. These additional accounts may be created post deployment using the `custAccounts` script.

System Manager Settings

Field	Information to enter	Notes
Primary System Manager IP	Enter the IP address of the primary System Manager that will be used to manage this Avaya Breeze® platform server.	
Enrollment Password	Enter the enrollment password that matches the value in System Manager administration.	You must know the enrollment password, and the password must not have expired. The password is set on System Manager at **Services › Security › Certificates › Enrollment Password**. On this page, verify that the **Time Remaining** value is greater than zero. If you do not know the password, create a new one.

Footprint values

Consult your Avaya Breeze® platform snap-in reference documents for specific profile and disk sizing requirements for the snap-ins you intend to install. Some snap-ins require higher disk space provisioning than the default of 50 GB. You must make this modification manually in the VM settings.

- Breeze 3.9 requires an additional 2 GB of memory per profile, as reflected in the table below.

Profile	CPU (cores)	Available Memory (GB)	Disk Storage (GB)	Maximum active SIP application sessions
1	4	8	50GB	29,900 sessions.
2	4	10		
3	6	12		44,880 sessions.

Table continues

Profile	CPU (cores)	Available Memory (GB)	Disk Storage (GB)	Maximum active SIP application sessions
4	8	18	50 GB	59,840 sessions.
5	12	29	For Solution Deployment Manager deployments, this increases to 150 GB.	90,000 sessions.

Virtual machine

The Avaya Breeze® platform profile you select has default values, which can be adjusted, for these settings.

Setting	Information to enter
CPU/Memory allocation and reservations	Consult your snap-in reference document for specific sizing requirements.
DataStore location	Select the datastore location to store the virtual machine files.
Host networking assignments	

Administering Avaya Aura® Media Server for REST

About this task

Use this procedure to configure Avaya Aura® Media Server to allow REST access using HTTP.

For more information, see *Implementing and Administering Avaya Aura® Media Server*.

Procedure

1. Log on to the Avaya Aura® Media Server web console.
2. Navigate to **System Configuration › Signaling Protocols › REST › General Settings**.
3. To enable TLS for REST services, select the **Enable TLS Transport** check box.
4. To enable two-way authentication for an extra level of security, select the **Enable TLS Mutual Authentication** check box.

5. To use plaintext usernames and passwords, select **Basic Authentication**. Alternatively, to include an authentication realm and encrypt the credentials before sending them over the network, select **Digest Authentication**.
   a. Enter the required username and password credentials in the **Authentication Username** and **Authentication Password** fields.
   b. If you selected **Digest Authentication**, then enter the name of the required authentication realm in the **Authentication Realm** field.
6. Click **Save**.

   Changes to the transport settings require a restart to take effect.
7. Navigate to **System Configuration › Network Settings › General Settings › Connection Security**.
8. Select the **Verify Host Name of TLS Client Connections** check box.
9. Change the **Minimum TLS Version** from **TLSv1.3** to **TLSv1.2**.
10. Click **Save**.
11. Navigate to **Security › Certificate Management › Key Store**.
12. Assign System Manager signed certificate to all service profiles.
13. Click **Save**.
14. Restart Avaya Aura® Media Server:
    a. Navigate to **System Status › Element Status**.
    b. Click **Restart**.

Assigning Avaya Aura® Media Server for use with Avaya Breeze® platform

Procedure

1. In System Manager, click **Elements › Media Server › Application Assignment**.
2. Select the check box next to Avaya Breeze® platform and click **Edit**.
3. Select the check box next to Avaya Aura® Media Server and click **Commit**.
   - The system takes up to two minutes to update the Avaya Breeze® platform.
   - You cannot assign Avaya Aura® Media Server to multiple applications.

Backing up the cluster database

About this task

The cluster database contains databases defined by the snap-ins installed on the cluster. You must take a backup to restore the databases after upgrading, or if it becomes necessary to roll back to the previous release.

- **If upgrading from pre-R3.9 servers:**

  If upgrading pre-R3.9 Avaya Breeze® platform to R3.9 or higher, you need to perform multiple backups:

a. Take a backup as detailed below. You can use this backup to restore the database if you need to roll back to the pre-3.9 release.
b. Install the clusterDBMigrationService-3.9.0.0 service.
c. After installing the clusterDBMigrationService-3.9.0.0 service, take another backup. You can use this backup to restore the database after upgrading.

Before you begin

- Windows servers are incompatible with the Cluster Backup and Restore feature and should not be used as an archive server.

Next steps

- You must now install the clusterDBMigrationService-3.9.0.0 service. After installing the service, you must take another backup. You can use the second backup to restore the cluster database after upgrading to R3.9 or higher.

Installing the clusterDBMigration service

About this task

Pre-R3.9 Servers Only

The clusterDBMigrationService is delivered and pre-loaded as part of Element Manager R3.9. The clusterDBMigration service is versioned as a 3.9 service, however the snap-in is compatible and intended to be installed on 3.8.1.1 and earlier Breeze clusters.

It should be installed onto the Avaya Breeze® platform R3.8.x cluster prior to the cluster server upgraded. This allows the existing cluster database backed up from R3.8.x to be restored to the cluster following the upgrade of the cluster servers to Avaya Breeze® platform R3.9.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Service Management › Services**.
2. Select the clusterDBMigrationService and click **Install**.
3. Select the clusters on which you want to install the clusterDBMigrationService and click **Commit**.
4. To see the status of the service installation, click **Refresh**.
    - **Installed** with a green check mark indicates that the snap-in has completed installation on all the Avaya Breeze® platform servers in the cluster.
    - **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all the servers.

Backing up the cluster database

About this task

Pre-R3.9 Servers only

If upgrading from pre-R3.9 Avaya Breeze® platform, you can only use the backup taken before installing the clusterDBMigrationService-3.9.0.0 service to roll back to the previous pre-R3.9 release.

For the upgrade process, you need to take another backup after having installed the migration service. You can use this backup to restore that database after upgrading.

Before you begin

- Install the "Installing the clusterDBMigration service" on page 28
- Windows servers are incompatible with the Cluster Backup and Restore feature and should not be used as an archive server.

Disabling the secure grid

About this task

Complete this procedure only if you have enabled the secure grid for a cluster. This procedure is service impacting.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Cluster Administration**.
2. Select the cluster that contains the servers you want to upgrade.
3. From the **Cluster State** drop-down menu, select **Deny New Service**.
4. Verify that the system displays **Denying** in the **Cluster State** column.
5. Select the cluster that contains the servers you want to upgrade and click **Edit**.
6. Under Cluster Attributes uncheck **Use secure grid?**
7. Click **Commit**.
8. Select the cluster that contains the servers you want to upgrade.
9. From the **Cluster State** drop-down menu, select **Accept New Service**.

Downloading software from PLDS

Procedure

1. On your web browser, type http://plds.avaya.com to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS Home page, select **Assets**.
4. Click **View Downloads**.
5. Click the search icon for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type Avaya or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.

- In the **Application** field, click the application name.

8. Click **Search Downloads**.
9. In the **Download Manager** box, click the appropriate **Download** link.

> **Note:**
>
> The first link, **Click to download your file now**, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The **click here** link uses your standard browser download and does not provide the download integrity features.

10. If you use the Download Manager, click **Details** to view the download progress.
11. Select a location where you want to save the file, and click **Save**.
12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Verifying the enrollment password status

The Avaya Breeze® platform requires an Enrollment Password during the initial installation and deployment process. Enrolling a password establishes trust between System Manager and Avaya Breeze® platform. The enrollment password is also known as the 'certificate enrollment password'.

- If the enrollment password has expired, renew the existing password.
- If the **Time Remaining** value is not zero, the password is valid. Verify that the time remaining is sufficient.

Procedure

1. In System Manager, click **Services › Security › Certificates › Enrollment Password**.
2. If the value of the **Time Remaining** field is zero, renew the password:
   a. In the **Password expires in** field, select a value from the drop-down menu for the time when the password must expire.
   b. Enter the password in the **Password** field.
   c. Reenter the password in the **Confirm Password** field.
   d. Click **Commit**.

   The system updates the **Time Remaining** field.

Verifying the signature algorithm of their existing LDAP/LDAPS server certificate

Procedure

1. Run the command: openssl s_client -connect <LDAP-FQDN>:636 -servername <LDAP-FQDN> </dev/null 2>/dev/null | openssl x509 -noout -text | grep -i "Signature Algorithm"

For example, if LDAP server FQDN is server.example.com, command is:

```
openssl s_client -connect server.example.com:636 -servername puneccq01.puneccq.avaya.com
</dev/null 2>/dev/null | openssl x509 -noout -text | grep -i "Signature Algorithm"
```

If the existing LDAP certificate is RSA 2048 / SHA256WITHRSA, no certificate renewal is required for the Breeze 3.9.0.4 upgrade.

If the existing LDAP certificate is RSA 2048 / SHA1WITHRSA, the customer must follow their respective CA/certificate-management procedure to generate and install a new RSA 2048 / SHA256WITHRSA LDAP server certificate before upgrading to Avaya Breeze 3.9.0.4.

2. Generate/reissue an RSA 2048 / SHA256WITHRSA certificate using the respective CA procedure and do the following:
   a. Install the certificate on the LDAP server.
   b. import the required new LDAP/CA certificate into the Authorization Service trusted store on the Breeze node(s) And System Manager Element.

      For information about importing LDAP server certificate, see "LDAP server certificate " in *Administering Avaya Breeze*.
   c. Verify LDAPS connectivity and proceed with Breeze 3.9.0.4 upgrade.

After installing the new certificate, the customer should verify that the LDAP server presenting the new certificate on port 636.

Note:

LDAP certification SHA-1 algorithm no longer supports on Avaya Breeze 3.9.0.4.

Setting the cluster to Deny New Service status

About this task

Place the cluster in the **Deny New Service** state before you edit the cluster attributes.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the cluster that you want to upgrade.
4. From the **Cluster State** drop-down menu, select **Deny New Service**.
5. Verify that the system displays `Denying` in the **Cluster State** column.

Verifying there is no server activity

About this task

You must verify that there is no activity on the Avaya Breeze® platform servers in the cluster before continuing with upgrading.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Cluster Administration**.
3. In the row for the cluster you are upgrading, look at the **Activity** column.
4. Verify that the **Activity** is 0.
    - You can view the **Activity** for individual servers in the cluster by clicking **Show** in the **Details** column.
    - After stopping new services, it can take a couple of hours for activity to reach zero. If activity has not stopped in a reasonable time, you can choose to proceed with the upgrade. Active calls will continue, but snap-in call control stops.

Uninstalling and deleting snap-ins

About this task

Uninstall the Analytics Collector Snap-in and Engagement Call Control from the cluster. Also refer to the snap-in documentation for guidance on other snap-ins that you must remove before upgrading.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Service Management › Services**.
3. On the Service Management page, select the snap-in that you want to remove.
4. Click **Uninstall**.
5. Select the cluster or clusters from which you want to remove the snap-in.
    - You cannot uninstall a required snap-in from a cluster unless you have already installed another version of the required snap-in in the cluster.
    - The snap-in status shown on the Service Management page is an aggregated status of snap-in installation across all clusters. Therefore, the status remains **Installed** if you have the snap-in still installed on another cluster.
6. Select **Do you want to delete the database?** check box to delete the snap-in database.
7. On the Service Management page, select the service that you want to delete.
8. Click **Delete**.
    - Verify that the service is in the **Loaded** state before you click **Delete**.
9. In the Delete Service Confirmation dialog box, select the **Please Confirm** check box.
10. Click **Delete**.

Removing the existing servers from the cluster

About this task

This procedure is service impacting for the targeted cluster. It should only be performed during a scheduling maintenance if possible.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. Click **Cluster Administration**.
3. Select the targeted cluster and click **Edit**.
4. Navigate to the **Servers** tab.
5. For a single node cluster:
   a. Select the Avaya Breeze® platform server by selecting the blue **X** next to the assigned server.
   b. click **Commit**.
6. **For a two-node cluster:**
   a. On the **General** tab, under **Cluster Attributes**, disable **Load Balancer** if enabled.
   b. On the **General** tab, disable **Enable Database Auto Switchover** if enabled.
   c. If using the cluster database feature:
      a. Remove the standby server by choosing the blue **X** next to the server designated as **S** (standby).
      b. Remove the active server by choosing the blue **X** next to the server designated as **A** (active).
      c. Click **Commit**.
7. **For a cluster with more than three nodes:**
   a. On the **General** tab, disable **Enable Database Auto Switchover** if enabled.
   b. If using the cluster database feature:
      a. Remove the server instances without an **A** or **S** designation by choosing the blue **X** next to those servers.
      b. Remove the standby server by choosing the blue **X** next to the server designated as **S** (standby).
      c. Remove the active server by choosing the blue **X** next to the server designated as **A** (active).
      d. Click **Commit**.
8. Confirm the warnings presented regarding the service disrupting actions that will follow.
9. Wait until all services are successfully uninstalled.

Next steps

Shut down the servers.

Shutting down the existing servers

About this task

You must shut down all the existing old release servers in the cluster before beginning the OVA deployment of the new release servers.

- If resources allow, rename and retain the old server images until the upgrade is complete.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
2. Click the button in front of a server in the cluster.
3. From the **Shutdown System** drop-down menu, select **Shutdown**.
4. Repeat for every server in the cluster.

Deploying the replacement upgrade release servers

Use one of the following methods to deploy replacement servers using the new release OVA.

- You can deploy the OVA sequentially for each server in the cluster, or for all servers simultaneously.

Deploying Avaya Breeze® platform OVA with VMware vSphere Client connected to vCenter

Before you begin

The steps in this procedure use the vSphere Client connected to VMware vCenter. This method of deployment is available if vCenter version is 6.0 or earlier.

- Save the Avaya Breeze® platform OVA file onto the workstation running the vSphere Client.

Procedure

1. Log in to the vCenter using the VMware vSphere Client.
2. Click **File › Deploy OVF Template**
3. Click **Browse** and find the Avaya Breeze® platform OVA. Click **Next**.
4. Verify that the details displayed match the version of the Avaya Breeze® platform that you are expecting to deploy.
    - If the details do not match, you may have chosen the wrong OVA. Click **Back** and choose the correct OVA.
    - If the details match, click **Next**.
5. If you wish to accept the End User License Agreement click **Accept**, then click **Next**.
6. On the **Name and Location** page, enter a name for the Avaya Breeze® platform virtual machine. Select the inventory location for your virtual machine, then click **Next**.
7. On the **Deployment Configuration** page, select the configuration profile that best fits the deployment, then click **Next**.
8. On the **Host/Cluster** page, select the specific host on which you want to deploy this VM, and click **Next**.
9. On the **Disk Format** page, select the disk provisioning format you want, then click **Next**.
10. On the **Network Mapping** page, select the destination network for each Avaya Breeze® platform interface, and click **Next**.

11. On the **Properties** page, enter the configuration details for your new server. See the *Customer Configuration Information* you collected for the values to enter in these fields. Click **Next**.
12. On the **Ready to Complete** page, verify the listed properties.
    - If the values are incorrect, click **Back** to modify the values.
    - If the values are correct, click **Finish**.

    A status window pops up after clicking **Finish**. Wait for the deployment to complete. The time this takes depends on the speed of your network connection. Once completed, you can close the window.
13. Locate your new VM in the inventory list in the **vSphere Client** window, right click and click **Virtual Machine › Power › Power On**.

    Important:

    - If installing multiple servers, allow at least 5 minutes between starting each of the new virtual machines.

14. (Optional) To open a **console** window to your VM, right-click the VM and click **Open Console**.

Deploying Avaya Breeze® platform OVA with VMware vSphere Web Client

Before you begin

The steps in this procedure use vSphere Web Client connected to vCenter. It runs in a web browser.

- Save the Avaya Breeze® platform OVA file onto the workstation running the vSphere web client.

Procedure

1. If using vCenter 7.0 U2 or later, do the following.
   a. Download the OVF/OVA signing certificate chain from https://web.entrust.com/root-certificates/entrust_g2_ca.cer?_ga=2.204957712.1460439918.1633458407-705405935.1632328263. For more information, see the VMware article at https://kb.vmware.com/s/article/84240.
   b. Log in to vCenter as administrator.
   c. Click **Administration › Certificates › Certificate Management**.
   d. Click **Add** next to **Trusted Root Certificates**.
   e. Browse and select the certificates file downloaded in the first sub-step.
   f. Select the **Start Root certificate push to vCenter Hosts** check box.
2. Log in to the vCenter using the VMware vSphere Web Client.

   The format is `https://<IP Address:9443>/vsphere-client`
3. In the navigation pane, click **vCenter**.

4. Click **Inventory Trees › Hosts and Clusters**.
5. Expand **Hosts and Clusters** to locate and select the target deployment host.
6. Right-click the on the host and select **Deploy OVF Template**.
7. On the **Select Source** page, enter the **URL** or path for installing the OVA, and click **Next**.
8. On the **Review Details** page, confirm the properties of the OVA file you selected and click **Next**.
9. If using vCenter 7.0 U2 or later:
    - If you performed step 1: Ignore the "invalid certificate" warning in the **Publisher** field.
    - If you performed step 1: Click **Ignore** next to the warning "The certificate is not trusted".
10. To accept the End User License Agreement, click **Accept**.
11. Click **Next**.
12. Enter a name for the Avaya Breeze® platform VM and select the required datacenter folder for the VM.
13. Click **Next**.
14. On the **Select a resource** page, select the location to run the deployed template and click **Next**.
15. Select the configuration profile that best fits the deployment and click **Next**.
16. Select the virtual disk format you want and click **Next**.
17. Select the destination network for each Avaya Breeze® platform interface and click **Next**.
18. On the **Setup networks** page, configure the network settings for your VM and click **Next**.
19. On the **Customize template** page, enter the configuration details for your VM and click **Next**.
20. On the **Ready to Complete** page, verify the options for the VM:
    - If the values are incorrect, click **Back** to make the changes.
    - If the values are correct, click **Finish**.

    Wait for the deployment to complete. The time taken depends on the speed of your network connection.

    After the deployment is complete, the system updates the **Inventory list** and displays the new virtual machine.
21. Select the new VM and click the **Summary** tab.
22. Click **Actions › Power On**.

Important:

- If installing multiple servers, allow at least 5 minutes between starting each of the new virtual machines.

23. Click **Summary › Launch Console** to open a new console.

    The system displays the progress of the VM system initialization.

24. After the VM initialization is complete, log in by using the customer account that you set up earlier.

Deploying Avaya Breeze® platform OVA with VMware vSphere Client connected to ESXi host

Before you begin

The steps in this procedure use the VMware vSphere Client connected to the ESXi host.

- Save the Avaya Breeze® platform OVA file onto the workstation running the vSphere Client.

Procedure

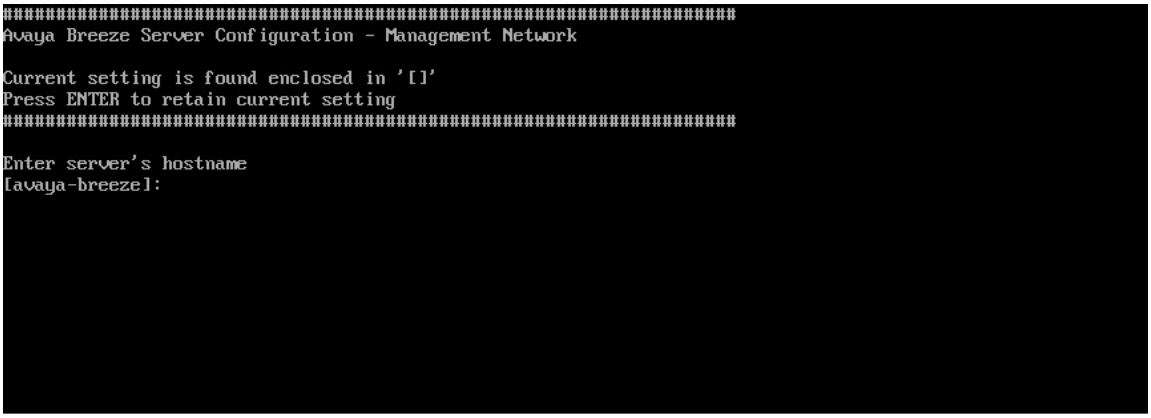
1. Log in to the VMware host using the VMware vSphere client.
2. Click **File › Deploy OVF Template**
3. Click **Browse** and find the Avaya Breeze® platform OVA.
4. Click **Next**.
5. Verify that the details displayed match the version of the Avaya Breeze® platform that you are expecting to deploy.
   - If the details do not match, you may have chosen the wrong OVA. Click **Back** and find the correct OVA.
   - If the details do match, click **Next**.
6. If you accept the End User License Agreement, click **Accept** and then click **Next**.
7. Enter a name for the Avaya Breeze® platform Virtual Machine (VM) on the **Name and Location** page and click **Next**.
8. On the **Deployment Configuration** page, select the configuration profile that best fits the deployment and click **Next**.
9. On the **Disk Format** page, select the disk provisioning format you want and click **Next**.

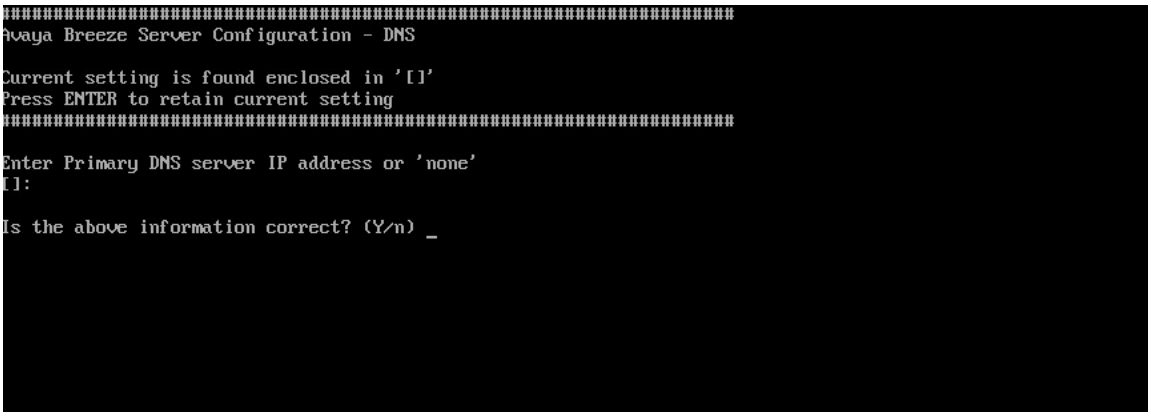
   While Avaya Breeze® platform works with either thick or thin provisioned disk, Avaya recommends using a **Thick Provision Lazy Zeroed** disk.

10. On the **Network Mapping** page, select the destination network for each Avaya Breeze® platform interface, then click **Next**.
11. On the **Ready to Complete** page, verify the options listed.
    - If the values are incorrect, click **Back** to modify the values.
    - If the values are correct, click **Finish**.

12. A status window pops up after clicking **Finish**. Wait for the deployment to complete. The time this takes depends on the speed of your network connection. After completing, close the window.
13. Locate your new VM in the **inventory list** in the **vSphere Client** window.
14. Right-click to go to **Power › Power On**.
15. To open a **console** window to your VM, right-click the VM and click **Open Console**.
16. During the boot, you will see the **End User License Agreement**. Scroll down through this document using the spacebar. At the bottom, enter `yes` if you agree to the terms.
17. When prompted to configure the virtual machine enter `y`.
18. Enter the management interface network parameters, date and time information, customer user information, and System Manager information.

    Refer to the following screenshots.





```
################################################################################
Avaya Breeze Server Configuration - PROXY

Current setting is found enclosed in '[]'
Press ENTER to retain current setting
################################################################################

Would you like to configure an HTTP proxy? (Y/n) _
```

```
Avaya Timezone Selection
                                                    America/Belem
                                                   America/Belize
                                                America/Blanc-Sablon
                                                  America/Boa_Vista
                                                   America/Bogota
                                                    America/Boise
                                                America/Buenos_Aires
                                                America/Cambridge_Bay
                                                America/Campo_Grande
                                                   America/Cancun
                                                   America/Caracas
                                                  America/Catamarca
                                                   America/Cayenne
                                                   America/Cayman
                                                   America/Chicago
                                                  America/Chihuahua
                                                America/Coral_Harbour
```

```
################################################################################
Avaya Breeze Server Configuration - Date/Time

Current setting is found enclosed in '[]'
Press ENTER to retain current setting
################################################################################

Select Timezone
[America/Denver]: America/Denver

Enter Date in MM/DD/YYYY format (i.e. 12/25/2008)
[08/25/2016]:

Enter Time in HH:MM 24 hour clock format (i.e. 13:30)
[02:12]:


Is the above information correct? (Y/n) _
```

```
Checking network connections...
VFQDN supplied: doctsmgr.doctsmgr.avaya.com
No network changes.
Reconfiguring platform                                  [  OK  ]
Reconfiguring jboss                                     [  OK  ]
Reconfiguring trust                                     [  OK  ]
Reconfiguring WebSphere                                 [  OK  ]
Reconfiguring DRS                                       [  OK  ]
Reconfiguring arbiter                                   [  OK  ]
Reconfiguring SAL                                       [  OK  ]
Reconfiguring ISMBus                                    [  OK  ]
Reconfiguring misc                                      [  OK  ]


Enter the Enrollment Password that matches the value in System
Manager administration (Security -> Certificates --> Enrollment Password).
Enrollment Password:
```

19. Run the `CEnetSetup` command to change the value of any OVA property specified during deployment.

Deploying Avaya Breeze® platform OVA with Solution Deployment Manager

This procedure uses the Solution Deployment Manager.

Before you begin

- Install the Avaya Aura® Appliance Virtualization Platform if necessary.
- Download the Avaya Breeze® platform OVA file.

Procedure

1. Copy the previously downloaded Avaya Breeze® platform OVA file to the System Manager `/swlibrary/staging/sync/` directory. If necessary, add the `staging/sync` folders to the directory structure.
2. In System Manager, click **Services › Solution Deployment Manager › Software Library Management**.
3. Click **Manage Files**.
4. In the list of **Sync Files from directory**, enter the SHA256 checksum and select a software library.
5. In **Product Family**, select **Avaya Breeze**.
6. In **Device Type** and **Software Type**, select **OVA**.
7. Click **Sync** and wait for the operation to complete.
8. Verify completion of the file sync to the library.
   a. Navigate to **Home › Services › Scheduler › Completed Jobs**.
   b. Check for `Job Name = IUM_syncFiles`, and `Job Status = SUCCESSFUL`.
9. Navigate to **Home › Services › Solution Deployment Manager › Software Library Management**.
10. Check SMGR_DEFAULT_LOCAL, click **Manage Files**, and confirm that the OVA file is in the list of files under **Software Library Files**.
11. Add a location to Solution Deployment Manager. There might be an existing location if adding a second or later virtual machine.
    a. On System Manager, click **Services › Solution Deployment Manager**.
    b. Click **Application Management**.
    c. Select **New** under **Locations**.
    d. Populate the location properties and click **Save**.
12. Add a host to a location. The VMware host or AVP must be accessible to the System Manager to perform this step.
    a. In the **Application Management Tree**, select the location to add the host to.
    b. Click the **Platforms** tab.
    c. Click **Add**.

d. Populate the **Host Name**, **Host FQDN or IP**, **User Name**, and **Password** fields using the same information used for the Appliance Virtualization Platform.

   For the **Host FQDN or IP** field, use the FQDN of the VMware host or the FQDN of the Appliance Virtual Platform.

13. Navigate to **Home › Services › Solution Deployment Manager › Application Management**.
14. Expand the **Application Management Tree** and expand the **Location**. Click the platform on which you want to deploy the Avaya Breeze instance.
15. On the **Applications** tab click **New**.
16. In the **Select Location and Platform** section, perform the following steps:

    Alternatively, in Step 12a, you can pre-select the location and platform in the **Application Management Tree**.

    a. In **Select Location**, select a location.
    b. In **Select Host**, select a host.
    c. Select a data store.

17. Click **Next**.
18. In the **Deploy OVA** section, perform the following steps:

    a. Select the **Select from software library** field.
    b. In the **Select Software Library** field, select the local and remote library where the OVA file is available. To deploy the OVA file using the Solution Deployment Manager client, use the default software library that is set during client installation.
    c. In **Select OVAs**, select the OVA file that you want to deploy.
    d. In **Flexi Footprint**, select a footprint.

       For more information, refer to the **Flexi Footprint** values in the "Key customer configuration information" section.

19. Click the **Network Parameters** tab and select appropriate networks.

    - Select the network that provides the subnet that Avaya Breeze® platform needs for SIP traffic (security module).
    - Select the network that provides the subnet that Avaya Breeze® platform needs for the management interface (Avaya Breeze® platform instance).

20. Click the **Configuration Parameters** tab and populate the Configuration Parameters fields.

> **Note:**
>
> The SIP entity name must match the VM name when deploying with Solution Deployment Manager.

21. Optionally on the **Configuration Parameters** tab, set up a customer root access account.

    a. Click the box to **Enable Customer Root Account for this Application**.

b. Click **Accept** to accept the **Root Access Acceptance Statement**.
c. Enter the **Customer Root Password**.

22. Click **Deploy** to begin the OVA deployment.
23. Click **Accept** to accept the license terms.
24. Click the **Virtual Machines** tab.
25. Click the **Status Details** link to display the **VM deploy Status** window. The deployment is complete when all status checks display green check marks.

Configure the new server automatic startup settings

For OVA deployments not using Solution Deployment Manager, you must configure all the Avaya Breeze® platform virtual machines to start automatically after the vSphere ESXi host starts.

- For Solution Deployment Manager deployment, automatic startup configuration is part of the VM deployment, you do not need to configure the virtual machine automatic startup settings.
- In high availability (HA) clusters, the VMware HA software ignores the startup selections.
- It is recommended to have a 5 minute delay between the startup of each of the servers.

Configuring virtual machine automatic startup settings using vSphere desktop client

Before you begin

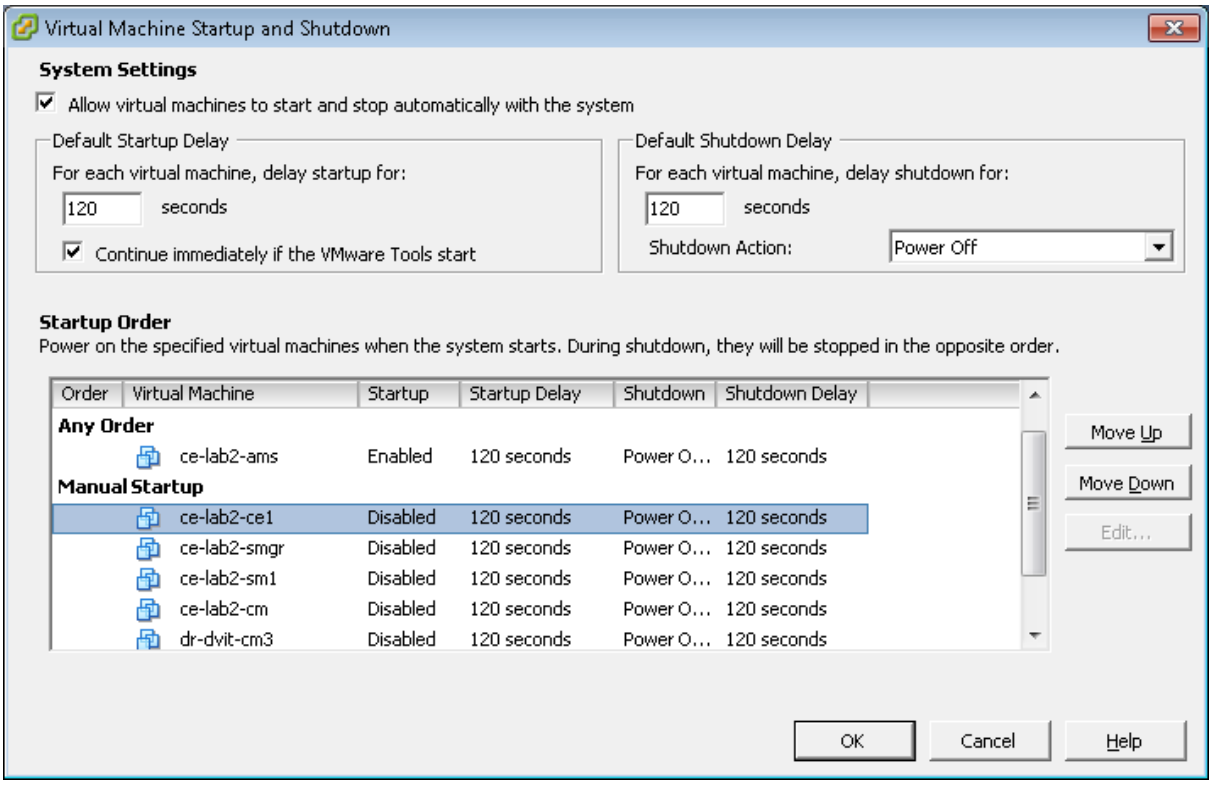
Confirm that you have the proper level of permissions to configure the automatic startup settings. If you do not have the proper level of permissions, contact your system administrator.

Procedure

1. In the vSphere Client inventory, select the host where the virtual machine is located.
2. Click the **Configuration** tab.
3. In the **Software** section, click **Virtual Machine Startup/Shutdown**.
4. Click **Properties** in the upper right corner of the screen.
5. In the **System Settings** section, select **Allow virtual machines to start and stop automatically with the system**.
6. In the **Default Startup Delay** section, set the **For each virtual machine, delay startup for** setting to 300 seconds. This setting is applied to the start time between each virtual machine set for automatic startup.
7. In the **Manual Startup** section, select the virtual machine.
8. Use the **Move up** button to move the virtual machine under **Automatic Startup**.
9. Click **OK**.

Example

The following is an example of the **Virtual Machine Startup/Shutdown** screen.



Configuring virtual machine automatic startup settings using vSphere Web Client

Before you begin

Confirm that you have the proper level of permissions to configure the automatic startup settings. If you do not have the proper level of permissions, contact your system administrator.

Procedure

1. Select the host where the virtual machine is located.
2. Click **Manage › Settings**.
3. Click **Virtual Machine Startup/Shutdown**.
4. Click **Edit**.
5. In the **System Settings** section, select **Allow virtual machines to start and stop automatically with the system**.
6. In the **Default Startup Delay** section, set the **For each virtual machine, delay startup for** setting to 300 seconds. This setting is applied to the start time between each virtual machine set for automatic startup.
7. In the **Manual Startup** section, select the virtual machine.
8. Move the Avaya Breeze® platform virtual machine to be included for **Automatic Startup**.

Changing the customer password on first login

Procedure

1. Log in to the deployed and configured Avaya Breeze® platform node.
2. Enter the customer login.
3. Enter the temporary customer password created while deploying the OVA.
4. When the system prompts to change the password for the customer login, enter the new password. The new password:
   - Must have at least eight characters.
   - Should not be based on a dictionary word or username.
   - Must contain a mix of numbers, letters, and at least one special character.
   - Must have a mix of upper and lower case letters.
   - Cannot be the same as the temporary password.
5. When the system prompts to confirm the password, reenter the same password that you entered above.

Creating multiple privileged user accounts

Procedure

1. Log in to Avaya Breeze® platform with the login credentials created during the OVA deployment.
2. Type the following command: **`custAccounts -a`**
3. When prompted to add this user as an EASG administrator, type **y** to enable the user to run EASG commands.
4. Enter the username and a temporary password for the new customer user account you are creating.

   The password is temporary. The server prompts the user to set a new password when they first login.

Installing the upgrade patch if required

About this task

This procedure provides general patching steps. For more information about specific patches, see *Avaya Breeze® platform Release Notes*.

⚠ Caution:

You cannot remove a patch after it is installed. This includes recovery from a patch install failing due to intermittent network issues. To enable recovery, you must take a snapshot of Avaya Breeze® platform before installing the patch. Verify that the system is running correctly after the patch is installed. When verified, remove the snapshot within 12–24 hours. See "VMware snapshots" on page 99 for special considerations when using snapshots.

Before you begin

- The server must be in the Deny New Service state.
- Ensure that the activity count is 0 for a cluster database.
- Download the patch file and copy it to the Avaya Breeze® platform server.
- The patch should have the following Linux permissions: `rw-r--r--`.

Procedure

1. Log in to Avaya Breeze® platform using the customer account.
2. Execute the `patchCE` command.

   For example: `$ patchCE –i /home/cust/<patchname>.bin`
3. When prompted that the patch is service interrupting, answer **Yes** and press `Enter`.

   The patch installs. Wait for the patch installation to complete. Depending on the patch, Avaya Breeze® platform may reboot.
4. Verify the version of the installed patch. The version can be viewed in one of the following ways:
   - Log in to Avaya Breeze® platform and execute the command `patchCE –s`.
   - Log in to Avaya Breeze® platform and execute the command `swversion`.
   - On System Manager, click **Elements › Avaya Breeze® › Server Administration**.
5. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
6. Identify the row for the Avaya Breeze® platform server you are patching and verify the following:
   - The **Service Install Status** is a green checkmark.
   - The **Security Module** is Up.
   - The **License mode** is a green checkmark.
   - The **Version** displays the new release.

Setting preferred snap-in version

About this task

You can set a preferred version of a snap-in.

- Non-call-intercept snap-ins automatically use the preferred version. Otherwise, they use the latest version of the snap-in.
- Service profile use the setting to indicate the version of the snap-in to provide to a group of users. Service profiles do not include non-call-intercept snap-ins.

For more information about service profiles and version designations, see *Administering Avaya Breeze® platform*.

Procedure

1. Designate the preferred version.
   a. On System Manager, click **Elements › Avaya Breeze® › Service Management**.

b. From the **All Services** list, select the version of the snap-in that you want to be the preferred version.
c. Click **Set Preferred Version**.
d. Select the clusters for which you want this to be the preferred version and click **Commit**.
    - You can set the preferred version for multiple snap-ins in a single transaction.

2. Edit the service profile.
    a. On System Manager, click **Elements › Avaya Breeze® › Configuration › Service Profiles**.
    b. Select the service profile and click **Edit**.
    c. Remove the snap-in from the service profile by clicking the **X** next to the snap-in name.
    d. In the list of **Available Service to Add to this Service Profile** click **Advanced** next to the snap-in name.
    e. For **Service Version** select **Preferred** and click **Add**.
    f. Click **Commit** to save the service profile.

Removing the clusterDBMigrationService

About this task

Pre- R3.9 Servers Only

The clusterDBMigrationService is only supported in a cluster of pre-R3.9 servers. After the servers have been upgraded to R3.9, you must remove the clusterDBMigrationService.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Service Management › Services**.
3. On the Service Management page, select the clusterDBMigrationService.
4. Click **Uninstall**.
5. From the Confirm Uninstall Service pop-up dialog box, select the cluster or clusters from which you want to remove the service

> **Note:**
>
> - The state of a snap-in as shown on the Service Management page is the aggregated status of the snap-in installation across clusters. If you uninstall a snap-in from one cluster, and it is still installed on another cluster, the status continues to display as **Installed**.

6. Check that the clusterDBMigrationService state now shows as **Loaded**.
7. Select the clusterDBMigrationService and click **Delete**.
8. In the Delete Service Confirmation dialog box, select the **Please Confirm** check box.
9. Click **Delete**.

Adding the new servers to the cluster

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. Click **Cluster Administration**.
3. Select the targeted cluster and click **Edit**.
   a. Navigate to the **Servers** tab.
   b. To add the Avaya Breeze® platform servers to the cluster, click **+** next to each unassigned server.
   c. Click **Commit**.
4. Wait until all services have installed.
5. To edit the cluster, on the **General** tab, under **Cluster Attributes**, enable **Load Balancer**.

Editing the cluster attributes

About this task

You can modify cluster attributes on the Cluster Editor page.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Cluster Administration**.
2. On the Cluster Administration page, select the upgraded cluster and click **Edit**.
3. On the Cluster Editor page, click the **General** tab.
4. Change the cluster name and IP address if required.
   a. Type a new cluster name.
   b. For load balancing, enter an IP address for the cluster in the **Cluster IP** field. This address must be a unique IP address on the same subnet as the Avaya Breeze® platform servers in the cluster.
5. Configure the cluster attributes.
   - By default, the cluster blocks HTTP traffic. To allow HTTP traffic in additional to HTTPS, uncheck **Only allow secure web communications**.
6. Click **Commit**.

Enabling the secure grid

About this task

Complete this procedure only if you had secure grid enabled for a cluster before the upgrade. This procedure is service impacting. Enabling secure grid will restart the cluster nodes individually during reconfiguration. It is advised to wait 10 minutes before rebooting the entire cluster to allow adequate time for this configuration to complete.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Cluster Administration**.

2. Select the cluster that contains the servers you upgraded.
3. From the **Cluster State** drop-down menu, select **Deny New Service**.
4. Verify that the system displays **Denying** in the **Cluster State** column.
5. Select the cluster that contains the servers you want to upgrade and click **Edit**.
6. Under Cluster Attributes select **Use secure grid**
7. Click **Commit**.
8. Select the cluster that contains the servers you upgraded.
9. From the **Cluster State** drop-down menu, select **Accept New Service**.

   For more information on **Use secure grid**, see the "Cluster Editor page field descriptions" section in the Administering Avaya Breeze® platform guide.

Verifying replication status

About this task

Complete this task to verify that the System Manager database has replicated to Avaya Breeze® platform.

Procedure

1. In System Manager, click **Services › Replication**.
2. Locate the Avaya Breeze® platform in the **Replica Group** list.
3. In the **Synchronization Status** column, verify that the Avaya Breeze® platform status is `Synchronized`.
   - Depending on the amount of data, the replication takes time to complete. Refresh the page periodically to check the status.
   - If the status is not `Synchronized`, for more information, see *Maintaining and Troubleshooting Avaya Breeze® platform*.

Running maintenance tests

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **System Tools And Monitoring › Maintenance Tests**.
3. In the **Select Avaya Breeze® to test** field, select an Avaya Breeze® platform server from the drop-down menu.
   a. To run all the tests, click **Execute All Tests**.
   b. To run specific tests: Select the test or tests that you want to run and then click **Execute Selected Tests**.

Verifying the status of the new servers

About this task

Verify that the Avaya Breeze® platform servers have upgraded and are functioning correctly.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
2. In the row for each Avaya Breeze® platform server in the cluster you are upgrading, verify that:
   - **Service Install Status** displays a green checkmark.
   - **Security Module** shows as Up.
   - **License mode** displays a green checkmark.
   - **Version** shows the expected new release number.

Installing new and upgraded snap-ins

About this task

Use this procedure to install new snap-ins on the upgraded cluster and to install new versions of updated snap-ins. Be sure to install the newest versions of connector snap-ins and the snap-ins that are mandatory for your cluster profile.

- The **Cluster Editor** page lists mandatory services for a cluster profile.
- For a list of connector snap-ins, see *Avaya Breeze® platform Overview and Specification*.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Service Management**.
2. Load the snap-in.
   a. Click **Load**.
   b. In the Load Service window, click **Choose file**, browse to select your snap-in and click **Open**.
   c. Click **Load** in the Load Service window.
   d. For licensed snap-ins, if you agree to the Avaya End User License Agreement (EULA), click **Accept**.

      Your snap-in displays on the Service Management page with a **State** of **Loaded**.
3. Install the snap-in.
   a. Select the snap-in you want to install.
   b. Click **Install**.
   c. Select the clusters where you want the snap-in to reside and click **Commit**.
   d. To see the status of the snap-in installation, click the **Refresh Table** icon located in the upper-left corner of the **All Services** list.
      - **Installed** with a green check mark indicates that the snap-in has completed installation on all Avaya Breeze® platform servers in the cluster.
      - **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all servers.

Restoring the cluster database

About this task

You can perform the restore process on any cluster which has the cluster database enabled.

Before you begin

- Enable the cluster database.
- Windows servers are incompatible with the Cluster Backup and Restore feature and should not be used as an archive server.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Cluster Administration**.
2. Click **Backup and Restore › Restore**. The system lists the backup and restore jobs.
3. Select a completed backup and then click **Restore**.
4. Select the cluster on which you want to restore the backup and then click **Continue**.

Rebooting a cluster

About this task

If using a multi-node node cluster, reboot the cluster after completing all the preceding process This ensure the data grid comes up properly.

Avaya Breeze® platform restarts all nodes in server clusters simultaneously when you restart clusters. You can view the progress of the cluster restart operation in the **Last reboot status** column on the **Server Administration** page of the System Manager web console.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the cluster and click **Cluster State › Deny New Service**.
4. When the system prompts, click **Continue**.
5. Select the cluster and click **Reboot**.
6. Click **Continue** when the system prompts.
    - The system reboots the cluster.
    - Reboot a cluster disabled **Database Auto Switchover** until you place the cluster back into **Accept New Service**.
    - You can view the reboot status in the **Last Reboot Status** column of **Cluster Administration**.

Adding a trusted certificate to all Avaya Breeze® platform servers in a cluster

Before you begin

Certificates that you intend to add as trusted certificates must be accessible in System Manager. For more information, refer to the *Deploying Avaya Breeze® platform* manual.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Cluster Administration**.
2. Select the cluster for which you want to administer the trusted certificates.
3. Click **Certificate Management › Install Trust Certificate (All Avaya Breeze® Instances)** to download the trusted certificates to all the servers in the cluster.
   - The trusted certificates that you add apply to all Avaya Breeze® platform servers assigned to the cluster.
4. From the **Select Store Type to install trusted certificate** menu, select the appropriate store type.
5. Click **Choose file** to navigate to the location of your trusted certificate, and then select the certificate.
6. Click **Retrieve Certificate** and review the details of the trusted certificate.
7. Click **Commit**.

Setting the cluster back to Accepting New Service status

About this task

After you have upgraded all the servers, you must return the cluster servers back to service from the **Cluster Administration** page. Do not return the servers back to service individually from the **Server Administration** page.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Cluster Administration**.
2. Click the checkbox in front of the upgraded cluster.
3. From the **Cluster State** drop-down menu, select **Accept New Service**.
4. Verify that the **Cluster State** column for the cluster changed to **Accepting**.

Verifying the Avaya Breeze® platform entity link connection

About this task

Use this procedure to verify that Session Manager can connect with Avaya Breeze® platform using the SIP entity link. You must verify the status of SIP link monitoring on the Session Manager instance.

Procedure

1. In System Manager, click **Elements › Session Manager › System Status › SIP Entity Monitoring**.
2. Click the name of the Session Manager instance that you linked to Avaya Breeze® platform.

   The system displays a list with the status of all entity links for the selected Session Manager.

3. Locate the Avaya Breeze® platform SIP entity and check **Conn. Status**.

   If you see UP, the link to Session Manager is successful. Otherwise, use the troubleshooting information in *Maintaining and Troubleshooting Avaya Breeze® platform*.

Chapter 5: Method 2: Upgrading using simultaneous cluster upgrade

You can use this method to simultaneously upgrade all nodes within a cluster within five minutes of each other.

You can perform this method of upgrading in the following ways:

- Using an ISO file.
- Using an OVA file through System Manager Solution Deployment Manager (SDM).

Checklist for upgrade method 2 - Simultaneous cluster upgrade

An ISO upgrade can fail due to networking and other problems outside the control of Avaya Breeze® platform. If that happens, and the ISO was complete and not truncated by the SFTP file transfer to the VM, you may be able to redo the upgrade.

- This method is not supported for upgrades to Avaya Breeze® platform R3.9 from earlier releases.

#	Action	Link/Notes	✔
1.	Check the prerequisites and post-upgrade tasks for snap-ins before proceeding with the upgrade.	Refer to the snap-in documentation.	

Table continues

#	Action	Link/Notes	✔
2.	Check whether Packetbeat or Metricbeat svar versions earlier than 3.9.0.4 are installed.	If found, uninstall the older Packetbeat and Metricbeat svars before upgrading Avaya Breeze® platform . Upgrading to Avaya Breeze platform 3.9.0.4 with older Packetbeat or Metricbeat still installed can cause error status on the Services page. To resolve this issue: 1. Uninstall the old Packetbeat and Metricbeat versions. 2. Install the newer Packetbeat and Metricbeat svar versions for 3.9.0.4 or later. 3. Confirm the installation status is healthy and the services are running.	
3.	Before upgrading Avaya Breeze® platform, upgrade the following in this order to the required release: 1. System Manager 2. Session Manager	See *Upgrading Avaya Aura® System Manager* and *Upgrading Avaya Aura® Session Manager*. If only upgrading the Avaya Breeze® platform Element Manager, use the **`upgradeSolution`** script. Refer to *Deploying Avaya Breeze® platform*.	
4.	Upgrade Avaya Aura® Media Server.	See *Deploying and Updating Avaya Aura® Media Server Appliance*. Upgrade Avaya Aura® Media Server within the same maintenance window as the Avaya Breeze® platform upgrade.	
5.	If you have a cluster database enabled, take a backup.	See *Administering Avaya Breeze® platform*.	

Table continues

#	Action	Link/Notes	✔
6.	To upgrade using the ISO file method, download the ISO file and patch file (if required) from PLDS. Confirm the files are complete by running checksum comparisons and then compare to the value on PLDS. If the file is correct, copy the ISO file and the patch file to each Avaya Breeze® platform server you will be upgrading. For upgrades using SDM: • Download the OVA file and patch file (if required) from PLDS. Confirm the files are complete by running checksum comparisons and then compare to the value on PLDS. • Download the versions*.xml file.	See "Downloading software from PLDS" on page 58 and "Downloading the version_edp.xml file" on page 65.	
7.	Install the Packetbeat and Metricbeat svars for version 3.9.0.4 or later. Verify that both services are running successfully from the Services page.	-	
8.	Verify that the enrollment password has not expired.	"Verifying Enrollment Password status" on page 59.	
9	Verify the signature algorithm of any existing LDAP/LDAPS server certificate.	"Verifying the signature algorithm of their existing LDAP/LDAPS server certificate" on page 30	
10.	Change the state of the cluster you are upgrading to **Deny New Service**.	"Denying new service" on page 60.	
11.	Update the Subject Alternative Name on the Manage Identity Certificate.	See "Updating the Subject Alternative Name on the Manage Identity Certificate" on page 60	
12.	Check the cluster **Activity** field is 0.	"Verify activity" on page 61.	

Table continues

#	Action	Link/Notes	✔
13.	Clear the **Enable Database Auto Switchover** field from **Elements › Avaya Breeze® › Cluster Administration**.	This step is only required for multi-node clusters with a Cluster database.	
14.	Take a snapshot of the current VM to enable reverting if necessary.	This task is not required if you are using SDM for the upgrade.	
15.	Uninstall the Analytics Collector Snap-in and Engagement Call Control from the cluster.	See the "Uninstalling a snap-in from a cluster" section in *Administering Avaya Breeze® platform*.	
16.	Edit the cluster and clear the **Pre-3.8.1 Cluster** cluster attribute.	See "Editing the cluster attributes" on page 47. You must perform all backups before changing the **Pre-3.8.1 Cluster** option.	
17.	Upgrade the Avaya Breeze® platform software.	To upgrade using the ISO file method, see "Upgrading the Avaya Breeze platform server" on page 61. To upgrade using SDM, see "Upgrades using Solution Deployment Manager" on page 61. The server reboots automatically when the upgrade script completes. Upgrade all nodes within the cluster simultaneously.	
18.	Install the patch file (if required) .	See "Patching the Avaya Breeze platform" on page 97.	
19.	Upgrade the mandatory snap-ins and connector snap-ins.	For more information, see your snap-in documentation.	
20.	Select the **Enable Database Auto Switchover** field from **Elements › Avaya Breeze® › Cluster Administration**.	This is only required for multi-node clusters with a cluster database.	

Table continues

#	Action	Link/Notes	✔
21.	Verify data replication between System Manager and Avaya Breeze® platform.	See "Verifying replication status" on page 70.	
22.	Run Avaya Breeze® platform maintenance tests for the server.	See "Running maintenance tests" on page 70. Resolve errors before proceeding. For information, see *Maintaining and Troubleshooting Avaya Breeze® platform*.	
23.	Install new snap-ins.	See "Installing new snap-ins" on page 72.	
24.	Set the preferred version for each snap-in.	See "Setting preferred snap-in version" on page 72.	
25.	Reboot the cluster.	Before the reboot, verify that **Service Install Status** shows a green checkmark for the cluster.	
26.	On the Server Administration page verify the following for the upgraded server: If using Reliable Eventing Framework, verify that the state of the node changes from Electing to Slave.	For more information, see "Verifying server status" on page 71.	
27.	Change the state to Accept New Service for the upgraded Avaya Breeze® platform cluster.	See "Accepting new service" on page 71.	
28.	Verify the Avaya Breeze® platform SIP entity link with Session Manager.	See "Verifying the Entity Link connection" on page 71.	
29.	Repeat steps 6 through 23 for each cluster that you are upgrading.	—	
30.	Test Avaya Breeze® platform snap-ins to verify that they are functioning correctly. Delete any snapshots that you no longer need.	It is important to delete snapshots you no longer need within 12–24 hours. For more information, see "VMware snapshots" on page 99.	

Table continues

#	Action	Link/Notes	✔
31.	Run a test alarm.	See the "Generating test alarms in System Manager" section in *Maintaining and Troubleshooting Avaya Breeze® platform*.	

Customer configuration information for ISO upgrades

You require the following information to upgrade Avaya Breeze® platform with an ISO file. Have this information before you begin the upgrade.

Customer login settings	Information to enter
Login Name	Enter the login ID to use for the customer account.
Enter Password	Enter the customer account password.

Downloading software from PLDS

About this task

Note:

You can download product software from https://support.avaya.com also.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon (🔍) for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type Avaya or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.

8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. On the PLDS page, get the md5sum and sha1sum.
    a. In the directory where you downloaded the ISO file, run the command: `md5sum aus-installer-correct version.iso`.
    b. Confirm that the checksum generated by this command matches the value on the PLDS page.
    c. If the values do not match, retry.
    d. If it fails again, contact Avaya Support.
12. If you receive an error message, click the message. Install ActiveX and continue with the download.
13. When the system displays the security warning, click **Install**.
    - When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Disabling the secure grid

About this task

Complete this procedure only if you have enabled the secure grid for a cluster. This procedure is service impacting.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Cluster Administration**.
2. Select the cluster that contains the servers you want to upgrade.
3. From the **Cluster State** drop-down menu, select **Deny New Service**.
4. Verify that the system displays **Denying** in the **Cluster State** column.
5. Select the cluster that contains the servers you want to upgrade and click **Edit**.
6. Under Cluster Attributes uncheck **Use secure grid?**
7. Click **Commit**.
8. Select the cluster that contains the servers you want to upgrade.
9. From the **Cluster State** drop-down menu select **Accept New Service**.

Verifying Enrollment Password status

Avaya Breeze® platform requires an Enrollment Password during the initial installation and deployment process. Enrolling a password establishes trust between the Breeze node and System Manager. The Enrollment Password is also known as the **certificate enrollment password**.

If the Enrollment Password has expired, renew the existing password for the upgrade to succeed.

If the **Time Remaining** is not zero, the password is valid. Verify that the time remaining is sufficient for the upgrade.

Procedure

1. In System Manager, click **Services › Security › Certificates › Enrollment Password**.
2. If the value of the **Time Remaining** field is zero, renew the password:
   a. In the **Password expires in** field, select a value from the drop-down menu for the time when the password must expire.
   b. Enter the password in the **Password** field.
   c. Reenter the password in the **Confirm Password** field.
   d. Click **Commit**.

   The system updates the **Time Remaining** field.

Denying new service

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
2. Select the server that you want to upgrade.
3. From the **System State** drop-down menu, select **Deny New Service**.
4. Verify that the system displays **Denying** in the **System State** column.

Updating the Subject Alternative Name on the Manage Identity Certificate

About this task

Before starting the upgrade, update the Subject Alternative Name (SAN) on the Manage Identity Certificate for each Breeze node in the cluster. The SAN must include the node's management IP address and `127.0.0.1`, as well as the node's management FQDN.

Procedure

1. Log in to System Manager at `https://<FQDN>/SMGR/` using valid credentials.
2. Go to **Services** → **Inventory** → **Manage Elements**.
3. Select the Breeze node.
4. From **More Actions**, select **Manage Identity Certificates**.
5. Select the management service, then click **Replace**.
6. In **Replace Identity Certificates**:
   a. Select **RSA** for Key Algorithm.
   b. Select the appropriate **Key Size**. For example, **2048**
   c. Under **Subject Alternative Names**, select **DNS Name** and **IP Address**.
   d. Ensure the IP Address field contains the node's management IP and 127.0.0.1, separated by a comma:

- If the field is empty, enter `<node management IP>,127.0.0.1`. For example, `10.92.18.231,127.0.0.1`
- If the field already contains the node's management IP, append `,127.0.0.1`. For example: `10.92.18.231,127.0.0.1`

e. Ensure the DNS Name field contains the node's management FQDN.

Example: `cc118131.avaya.com`

7. Click **Commit**.
8. Repeat these steps for every remaining Breeze node in the cluster.

Verify activity

About this task

Verify that there is no activity on the server you are upgrading.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
2. In the row for the server you are upgrading, look in the **Activity** column.
3. Verify that the **Activity** is 0.
   - It can take a couple of hours for activity to reach zero. If activity has not stopped in a reasonable time, you can choose to proceed with the upgrade. Active calls continue but without snap-in call control.

Upgrading the Avaya Breeze® platform server

Before you begin

1. Verify that you have copied the ISO upgrade file to the server that you are upgrading.
2. Take a snapshot of the current VM to enable reverting if necessary.

Procedure

1. Log on to the Avaya Breeze® platform server.
2. Enter the command **`upgradeCE`** *<iso filename>*.
3. Step through upgrade prompts.

Upgrades using Solution Deployment Manager

System Manager Solution Deployment Manager is a centralized upgrade solution, which you can use to upgrade Avaya Breeze® platform. You can upgrade from Avaya Breeze® platform Release 3.3 or higher to the latest release.

Solution Deployment Manager accesses the OVA file in the System Manager software library.

See the following documents for more information:

- *Upgrading and Migrating Avaya Aura® applications from System Manager*

- *Administering Avaya Aura® System Manager*
- *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*

Prerequisites

- To use the Solution Deployment Manager upgrade process, you must have Avaya Breeze® platform Release 3.3 or later.
- Check you can administer the VMware host or Appliance Virtualization Platform and the Avaya Breeze® platform virtual machine in Solution Deployment Manager Application Management. For more information, see *Administering Avaya Aura® System Manager*.

Checklist for upgrading Avaya Breeze® platform using Solution Deployment Manager

This checklist outlines the process to upgrade Avaya Breeze® platform using Solution Deployment Manager.

#	Task	✔
1	Complete items 1 to 13 in "Checklist for upgrade method 2 - Simultaneous cluster upgrade" on page 53.	
2	Ensure that you install Solution Deployment Manager.	
3	Install the OVA file into the System Manager software library.	
4	Upload the `versions_edp.xml` file to Solution Deployment Manager. For more information, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.	
5	Re-establish the trust connection when upgrading applications not deployed from Solution Deployment Manager.	
6	Refresh the host status.	
7	Refresh the elements. You can either run the job schedule immediately or schedule it for a later time.	
8	Analyze the software library inventory.	

Table continues

#	Task	✔
9	Perform the pre-upgrade check.	
10	Perform the upgrade using Solution Deployment Manager.	
11	Commit the upgrade of Avaya Breeze® platform.	
12	Copy the patch file to the Avaya Breeze® platform server.	
13	Return to item 15 in "Checklist for upgrade method 2 - Simultaneous cluster upgrade" on page 53.	

Installing the Solution Deployment Manager client

Procedure

1. Download the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.zip` file from the Avaya Support website at http://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.
2. On the Avaya Support website, click **Support by Products › Downloads**, and type the product name as **System Manager**, and Release as **8.0.x**.
3. Click the **Avaya Aura® System Manager Release 8.0.x SDM Client Downloads, 8.0.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

   You can also copy the zip file to your software library directory, for example, `c:/tmp/Aura`.
4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.
5. On the Welcome page, click **Next**.
6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.
7. On the Install Location page, perform one of the following:

   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.
   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

     To restore the path of the default directory, click **Restore Default Folder**.

   The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.
8. Click **Next**.

9. On the Pre-Installation Summary page, review the information, and click **Next**.
10. On the User Input page, perform the following:
    a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
    b. To change the default directory, in Select Location of Software Library Directory, click **Choose** and select a directory.

       The default software library of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts`.

       You can save the artifacts in the specified directory.
    c. In **Data Port No**, select the appropriate data port.

       The default data port is 1527. The data port range is from 1527 through 1627.
    d. In **Application Port No**, select the appropriate application port.

       - The default application port is 443. If this port is already in use by any of your application on your system, then the system does not allow you to continue the installation. You must assign a different port number from the defined range. The application port range is from 443 through 543.

       Note:

       After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.

    e. **(Optional)** Click **Reset All to Default**.
11. Click **Next**.
12. On the Summary and Validation page, verify the product information and the system requirements.

    - The system performs feasibility checks such as disk space and memory. If the system displays any error messages, you must make the required disk space, memory, or ports available to continue with installation.

13. Click **Install**.
14. To exit the installer, on the Install Complete page, click **Done**.

    The installer creates a shortcut on the desktop.
15. To start the client, click the Solution Deployment Manager client icon, .

Next steps

- If you are using the services port for the installation, configure the laptop to connect to the services port.
- Connect the Solution Deployment Manager client to Appliance Virtualization Platform through the customer network or services port.

  For information about "Methods to connect the Solution Deployment Manager client to Appliance Virtualization Platform", see *Using the Solution Deployment Manager client*.

Installing the OVA file into the software library

Procedure

1. Copy the previously downloaded Avaya Breeze® platform OVA file to the System Manager `/swlibrary/staging/sync/` directory.

   If necessary, add the `staging/sync` folders to the directory structure.
2. Navigate to **Home › Services › Solution Deployment Manager › Software Library Management** and click **Manage Files**.
3. In the Sync Files from directory list, enter the SHA256 checksum and select a software library.

   For **Product Family**, **Device Type**, and **Software Type**, select **others**.
4. Click **Sync** and wait for the operation to complete.
5. Verify the completion of the file sync to the library.
   a. Navigate to **Home › Services › Scheduler › Completed Jobs**.
   b. Look for Job Name = IUM_syncFiles, and Job Status = SUCCESSFUL.
6. Navigate to **Home › Services › Solution Deployment Manager › Software Library Management**.
7. To check SMGR_DEFAULT_LOCAL, click **Manage Files** and confirm that the OVA file appears in the list of files under Software Library Files.

Downloading the `version_edp.xml` file

About this task

This file provides information about your software entitlements.

Procedure

1. Log in to https://plds.avaya.com.
2. Search for the `smgr-versionsxmls.zip` using PLDS ID SMGRSUM0001:
   a. Click the **Assets** tab.
   b. Click **View Downloads**.
   c. Select **Search by Download**.
   d. In the **Download pub ID** field, enter `SMGRSUM0001`.
   e. Click **Search Downloads**.
3. Download the zip file.
4. Extract the zip file.

Re-establishing a trust connection

About this task

Use this procedure to reconnect applications not deployed from Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services › Solution Deployment Manager**.

2. In the navigation pane, click **Application Management**.
3. Select the virtual machine.
4. To establish trust, click **More actions › Re-establish connection**.
5. In the Select Version pane, select `others`.
6. Type the credentials and click **Reestablish Connection**.
    - The **Current Action Status** column displays the status of the virtual machine reestablishment.

Refreshing the host status

Procedure

1. In System Manager, click **Services › Solution Deployment Manager › Application Management**.
2. On **Application Management Tree**, click the required location.
3. Click the **Platforms** tab.

   The system displays the list of hosts for the selected location.
4. Select the required host.
5. Click **Refresh**.

   The **Current Action Status** column displays the status of the host.

Refreshing elements

About this task

Before upgrading, refresh elements on the Upgrade Management page.

Before you begin

On the User Settings page, configure the user settings.

Procedure

1. On the System Manager web console, click **Services › Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select one or more devices.
   b. Click **Pre-upgrade Actions › Refresh Element(s)**.
4. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
5. If you selected **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays ✔ and the **Current Version** column displays the current version of the element.

Analyzing software

About this task

Analyze the OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitlement upgrade version, the **Version** field must contain the appropriate value. You can get the version values from the `version_edp.xml` file you downloaded from PLDS.

You do not need to do this process for custom patching.

Before you begin

- On the Roles page, set the Software Management Infrastructure permission.
- Refresh elements.

Procedure

1. On the System Manager web console, click **Services › Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select a device that you want to analyze.
   b. Click **Pre-upgrade Actions › Analyze**.
4. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays a ✓, the Current Version column displays the current version of the element, and the Entitled Upgrade Version column displays the next version of the element which you can upgrade to.

Performing the pre-upgrade check

Procedure

1. On the System Manager web console, click **Services › Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select an application to upgrade.
   b. Click **Pre-upgrade Actions › Pre-upgrade Check**.
4. On the Pre-upgrade Configuration page, fill in the required information.

   To migrate to an ESXi host from the old server, in **Target Host**, select the ESXi host.
5. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.

6. Click **Schedule**.

   On the Upgrade Management page, the status of the **Last Action Status** and **Pre-upgrade Check Status** columns display a .

Upgrading Avaya Breeze® platform using Solution Deployment Manager

About this task

Use this procedure to upgrade Avaya Breeze® platform using Solution Deployment Manager.

Before you begin

Install the Solution Deployment Manager client.

Procedure

1. Do one of the following to access Solution Deployment Manager:
   - On the System Manager web console, click **Services › Solution Deployment Manager**.
   - Navigate to **Avaya › Avaya SDM Client** from the Windows **Start** menu.
   - Click the Solution Deployment Manager client icon ( ) on your desktop.
2. In the navigation pane, click **Upgrade Management**.
3. Click the Avaya Breeze® platform application to upgrade.
4. Click **Upgrade Actions › Upgrade/Update**.
5. On the Upgrade Configuration page, to view the devices associated with the application that you want to upgrade, do the following:
   a. Click **Details** and review the dependent devices.
   b. Click **Done**.
6. To continue with upgrade when the recommended checks fail during the pre-upgrade check, select the **Override pre-upgrade check** checkbox.
7. To provide the upgrade configuration details, click **Edit**.
8. To upgrade:
   a. Select the appropriate ESXi host.
   b. In the **Upgrade Source** field, select **SMGR_DEFAULT_LOCAL**.
   c. In the **Upgrade To** field, select the OVA file.
   d. In **Existing Administrative User**, type the customer login name.
   e. In **Existing Administrative Password**, type the customer login password.
   f. Click **Pre-populate Data**.

      The system populates the data for the following fields:

      - **IP Address**
      - **Short Hostname**
      - **Network Domain**
      - **Netmask**
      - **Default Gateway**
      - **DNS server(s)**

- **Timezone**
- **NTP server(s)**
- **Login Name**
- **Enter Customer Account Password**
- **Primary System Manager IP**
- **Enrollment Password**
- **Accept the License Agreement**

g. In the **Flexi Footprint** field, select the footprint based on the user requirement.

h. Do one of the following in the **EASG User Access** field:

- Type 1 to enable EASG.

  Avaya recommends that you enable EASG.
- Type 2 to disable EASG.

i. In the **Public** field, select the network that will support the Avaya Breeze® platform security module network.

j. In the **Out of Band Management** field, select the network that supports the Avaya Breeze® platform management network.

k. In the **Datastore** field, select the datastore that supports the Avaya Breeze® platform server.

l. Click **Save**.

9. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

   If the field displays , review the information on the Edit Upgrade Configuration page.

10. On the Upgrade Configuration page, click **Upgrade**.
11. On the Job Schedule page, click one of the following:

    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.

12. Click **Schedule**.
13. Click **Upgrade**.
14. To view the upgrade status, do the following:

    a. In the navigation pane, click **Upgrade Job Status**.

    b. In the **Job Type** field, click **Upgrade**.

    c. Click the upgrade job that you want to view.

15. Verify that the upgrade of the application is successful.

Committing the upgrade of Avaya Breeze® platform

Procedure

1. In System Manager, click **Services › Solution Deployment Manager › Upgrade Management**.

2. Select the Avaya Breeze® platform by selecting the check box to the left of the **Name** column.
3. In the **Upgrade Actions** menu, click **Commit/Rollback Upgrade**.

   The system displays the Job Schedule page.
4. Select **Commit** in the **Upgrade Actions** column.
5. Click **Run Immediately** to perform the job now or click **Schedule later** to perform the job at a scheduled time.
6. Click **Schedule**.

   The system returns to the Upgrade Management page.
7. Click **Enable Auto Refresh**.

   The system updates the **Last Action** and **Last Action Status** fields when the Commit job is complete.
8. Click the icon in the **Last Action Status** field.

   The system displays the Element Check Status dialog box.
9. Click **Done**.
10. To view the Commit job status, perform the following:
    a. In the navigation pane, click **Upgrade Jobs Status**.

       The system displays the Upgrade Jobs Status page.
    b. In the **Job Type** menu, click **Commit/Rollback Upgrade**.
    c. In the **Job Name** column, click the job that you want to view.
    d. Click **Done**.

Verifying replication status

About this task

Complete this task to verify that the Avaya Breeze® platform database replicated.

Procedure

1. In System Manager, click **Services › Replication**.
2. Locate the Avaya Breeze® platform in the **Replica Group** list.
3. In the **Synchronization Status** column, verify the status is `Synchronized`.

   If the status is not `Synchronized`, for more information, see *Maintaining and Troubleshooting Avaya Breeze® platform*.

Running maintenance tests

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **System Tools And Monitoring › Maintenance Tests**.
3. In the **Select Engagement Development Platform to test** field, select a server from the drop-down menu.

4. To run all the tests, click **Execute All Tests**.
5. To run specific tests:
   a. Select the test or tests that you want to run.
   b. Click **Execute Selected Tests**.

Verifying server status

About this task

Verify that the server has upgraded to release 3.1.1 and is functioning correctly.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
2. In the row for the server you are upgrading, verify the following information:
   - The **Service Install Status** is a green checkmark
   - The **Security Module** is Up
   - The **License mode** is a green checkmark
   - The **Version** displays release 3.1.1.

Accepting new service

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
2. Select the server and click **System State › Accept New Service**.
3. Verify that the **System State** column for the server changes to **Accepting**.

Verifying the Entity Link connection

About this task

Complete this task to verify that Session Manager can connect with Avaya Breeze® platform using the SIP Entity Link. To do this you must verify the status of SIP link monitoring on the Session Manager instance.

Procedure

1. In System Manager, click **Elements › Session Manager › System Status › SIP Entity Monitoring**.
2. Click the name of the Session Manager Instance that you linked to Avaya Breeze® platform.

   The system displays a list with the status of all the Entity Links for the selected Session Manager.
3. Locate the Avaya Breeze® platform SIP Entity and check the **Conn. Status** column.
   - If you see `UP`, the link to is successful.
   - If you do not see `UP`, for additional information, see *Maintaining and Troubleshooting Avaya Breeze® platform*.

Installing new snap-ins

About this task

Complete this procedure to install new snap-ins on the upgraded cluster and to optionally install new versions of updated snap-ins. Be sure to install the newest versions of connector snap-ins and the snap-ins that are mandatory for your cluster profile. The Cluster Editor page lists Mandatory services for a cluster profile.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Service Management**.
2. Load the snap-in.
   a. Click **Load**.
   b. In the Load Service window, click **Choose file**, browse to select your snap-in and click **Open**.
   c. Click **Load** in the Load Service window.
   d. For licensed snap-ins, if you agree to the Avaya End User License Agreement (EULA), click **Accept**.

      Your snap-in displays on the Service Management page with a **State** of **Loaded**.
3. Install the snap-in.
   a. Select the snap-in you want to install.
   b. Click **Install**.
   c. Select the clusters where you want the snap-in to reside and click **Commit**.
   d. To see the status of the snap-in installation, click the Refresh Table icon located in the upper-left corner of the **All Services** list.

      Installed with a green check mark indicates that the snap-in has completed installation on all servers in the cluster. **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all servers.

Setting preferred snap-in version

About this task

It is possible to set a preferred version of a snap-in. A service profile uses this to indicate the version of the snap-in to provide to a group of users. You must first designate the version of the snap-in that is the preferred version. Then, change the version designation for the snap-in in the service profile. For more information about service profiles and version designations, see *Administering Avaya Breeze® platform*.

Non-call-intercept snap-ins automatically use the preferred version if specified, otherwise they use the latest version. Service profiles do not include non-call-intercept snap-ins.

Procedure

1. Designate the preferred version.
   a. In System Manager navigate to **Home › Elements › Engagement Development Platform › Service Management**.

b. From the **All Services** list, select the version of the snap-in that you want to be the preferred version.
c. Click **Set Preferred Version**.
d. Select the clusters for which you want this to be the preferred version and click **Commit**.

2. Edit the service profile.

a. In System Manager navigate to **Home › Elements › Engagement Development Platform › Configuration › Service Profiles**.
b. Select the service profile and click **Edit**.
c. Remove the snap-in from the service profile by clicking the **X** next to the snap-in name.
d. In the list of **Available Service to Add to this Service Profile** click **Advanced** next to the snap-in name.
e. For **Service Version** select **Preferred** and click **Add**.
f. Click **Commit** to save the service profile.

Chapter 6: Method 3: Upgrading using rolling cluster upgrade

You can use this method to perform rolling upgrade of each node within a cluster in turn. This upgrade method is not service impacting.

- This method is not supported for upgrades to Avaya Breeze® platform R3.9 from earlier releases. Refer to Method 1, which outlines the supported upgrade procedure. For more informaton, see "Method 1: Upgrading using OVA reinstallation" on page 16.

  Note:

  This method is not supported for upgrades from R3.9.0.0 to higher releases. This method is supported for upgrades from R3.9.0.2 or later to higher releases.

- You can perform this method of upgrading in the following ways:
  - Using an ISO file.
  - Using an OVA file through System Manager Solution Deployment Manager (SDM).

Checklist for upgrade method 3 - Rolling cluster upgrade

An ISO upgrade can fail due to networking and other problems outside the control of Avaya Breeze® platform. If that happens, and the ISO was complete and not truncated by the SFTP file transfer to the VM, you may be able to redo the upgrade.

#	Action	Link/Notes	✔
1.	Check the prerequisites and post-upgrade tasks for snap-ins before proceeding with the upgrade.	Refer to the snap-in documentation.	

Table continues

#	Action	Link/Notes	✔
2.	Before upgrading Avaya Breeze® platform, upgrade the following in this order to the required release: 1. System Manager 2. Session Manager	See *Upgrading Avaya Aura® System Manager* and *Upgrading Avaya Aura® Session Manager*. If only upgrading the Avaya Breeze® platform Element Manager, use the **`upgradeSolution`** script. Refer to *Deploying Avaya Breeze® platform*.	
3.	Upgrade Avaya Aura® Media Server.	See *Deploying and Updating Avaya Aura® Media Server Appliance*. Upgrade Avaya Aura® Media Server within the same maintenance window as the Avaya Breeze® platform upgrade.	
4.	If you have a cluster database enabled, take a backup.	See *Administering Avaya Breeze® platform*.	
5.	On the Cluster Administration page, identify the cluster you want to upgrade. For clusters with multiple servers, determine the sequence in which you want to upgrade the servers.	See "Viewing and changing server cluster database status" on page 79 and "Server upgrade sequence" on page 78. This step is for upgrading Avaya Breeze® platform nodes with snap-ins that support non-service impacting upgrades. Check your snap-in documentation for specific upgrade considerations.	

Table continues

#	Action	Link/Notes	✔
6.	To upgrade using the ISO file method, download the ISO file and patch file (if required) from PLDS. Confirm the files are complete by running checksum comparisons and then compare to the value on PLDS. If the file is correct, copy the ISO file and the patch file to each Avaya Breeze® platform server you will be upgrading. For upgrades using SDM: • Download the OVA file and patch file (if required) from PLDS. Confirm the files are complete by running checksum comparisons and then compare to the value on PLDS. • Download the versions*.xml file.	See "Downloading software from PLDS" on page 79. For more information about SDM upgrades, see "Upgrades using Solution Deployment Manager" on page 61.	
7.	Verify that the enrollment password has not expired.	See "Verifying Enrollment Password status" on page 80.	
8.	Verify the signature algorithm of any existing LDAP/LDAPS server certificate.	"Verifying the signature algorithm of their existing LDAP/LDAPS server certificate" on page 30	
9.	Change the state of the cluster you are upgrading to **Deny New Service**.	See "Denying new service" on page 81.	
10.	Update the Subject Alternative Name on the Manage Identity Certificate.	See "Updating the Subject Alternative Name on the Manage Identity Certificate" on page 60	
11.	If a cluster database is enabled and the next node is an active node, change the status of the active node to Standby.	See "Viewing and changing server cluster database status" on page 79.	
12.	Verify that the server **Activity** field is set to 0.	See "Verify activity" on page 82.	
13.	Take a snapshot of the current VM to enable reverting if necessary.	This task is not required if you are using the SDM upgrade option.	

Table continues

#	Action	Link/Notes	✔
14.	Upgrade the Avaya Breeze® platform software.	To upgrade using the ISO file method, see "Upgrading the Avaya Breeze platform server" on page 82. For more information about SDM upgrades, see "Upgrades using Solution Deployment Manager" on page 61. The server reboots automatically when the upgrade script completes.	
15.	Install the patch file (if required).	See "Patching the Avaya Breeze platform" on page 97.	
16.	Upgrade the mandatory snap-ins and connector snap-ins.	For more information, see your snap-in documentation.	
17.	Verify data replication between System Manager and Avaya Breeze® platform.	See "Verifying replication status" on page 91.	
18.	Run Avaya Breeze® platform maintenance tests for the server.	See "Running maintenance tests" on page 91. Resolve errors before proceeding. For information, see *Maintaining and Troubleshooting Avaya Breeze® platform*.	
19.	On the Server Administration page verify the following for the upgraded server: If using Reliable Eventing Framework, verify that the state of the node changes from Electing to Slave.	See "Verifying server status" on page 92. Complete this procedure only if you have disabled secure grid for the cluster that contains the servers you are upgrading. This procedure is service impacting.	
20.	Change the state to Accept New Service for the upgraded Avaya Breeze® platform node.	See "Accepting new service" on page 92.	
21.	Verify the Avaya Breeze® platform SIP entity link with Session Manager.	See "Verifying the Entity Link connection" on page 92.	

Table continues

#	Action	Link/Notes	✔
22.	Repeat steps 7 through 17 for each cluster you are upgrading.	—	
23.	Install new snap-ins.	See "Installing new snap-ins" on page 93.	
24.	Set the preferred version for each snap-in.	See "Setting preferred snap-in version" on page 93.	
25.	Test Avaya Breeze® platform snap-ins to verify that they are functioning correctly. Delete any snapshots that you no longer need.	It is important to delete snapshots you no longer need within 12–24 hours. For more information, see "VMware snapshots" on page 99.	
26.	Run a test alarm.	—	

Customer configuration information for ISO upgrades

You require the following information to upgrade Avaya Breeze® platform with an ISO file. Have this information before you begin the upgrade.

Customer Login Settings

Field	Information to enter	Notes
Login Name	`Enter Login ID to use for the customer account`.	Login ID and password for customer account you will use during deployment
Enter Password	`Enter the customer account password.`	

Server upgrade sequence

If you have multiple servers in a cluster and have snap-ins that use the cluster database, you must upgrade the servers in the correct sequence to avoid data loss. The sequence depends on the active, standby, or idle status of the server. View the status on the System Manager Avaya Breeze® platform Cluster Administration page.

Upgrade sequence

1. Upgrade all idle servers.

2. Upgrade the standby server.
3. Switch the active server to be the standby server. (The standby server becomes the new active server.)
4. Upgrade the new standby server.

Viewing and changing server cluster database status

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Cluster Administration**.
2. Click **Show** in front of the cluster that contains the servers you are upgrading.
3. In the Cluster Database column, identify the Active, Standby, and Idle servers.
4. To change the server cluster database status, click the status in the Cluster Database column.
    - Active status changes to standby
    - Standby status changes to active
    - Idle status changes to standby

Downloading software from PLDS

About this task

Note:

You can download product software from https://support.avaya.com also.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon () for Company Name.
6. In the Search Companies dialog box, do the following:
    a. In the **%Name** field, type Avaya or the Partner company name.
    b. Click **Search Companies**.
    c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
    - In **Download Pub ID**, type the download pub ID.
    - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file and click the **Download** link.

10. Select a location where you want to save the file and click **Save**.
11. On the PLDS page, get the md5sum and sha1sum.
    a. In the directory where you downloaded the ISO file, run the command: `md5sum aus-installer-correct version.iso`.
    b. Confirm that the checksum generated by this command matches the value on the PLDS page.
    c. If the values do not match, retry.
    d. If it fails again, contact Avaya Support.
12. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
13. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Disabling the secure grid

About this task

Complete this procedure only if you have enabled the secure grid for a cluster. This procedure is service impacting.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Cluster Administration**.
2. Select the cluster that contains the servers you want to upgrade.
3. From the **Cluster State** drop-down menu, select **Deny New Service**.
4. Verify that the system displays **Denying** in the **Cluster State** column.
5. Select the cluster that contains the servers you want to upgrade and click **Edit**.
6. Under Cluster Attributes uncheck **Use secure grid?**
7. Click **Commit**.
8. Select the cluster that contains the servers you want to upgrade.
9. From the **Cluster State** drop-down menu, select **Accept New Service**.

Verifying Enrollment Password status

Avaya Breeze® platform requires an Enrollment Password during the initial installation and deployment process. Enrolling a password establishes trust between System Manager and the Avaya Breeze® platform. The Enrollment Password is also known as the **certificate enrollment password**.

If the Enrollment Password has expired, renew the existing password for the upgrade to succeed.

If the **Time Remaining** is not zero, the password is valid. Verify that the time remaining is sufficient for the upgrade.

Procedure

1. In System Manager, click **Services › Security › Certificates › Enrollment Password**.
2. If the value of the **Time Remaining** field is zero, renew the password:
   a. In the **Password expires in** field, select a value from the drop-down menu for the time when the password must expire.
   b. Enter the password in the **Password** field.
   c. Reenter the password in the **Confirm Password** field.
   d. Click **Commit**.

   The system updates the **Time Remaining** field.

Denying new service

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
2. Select the server that you want to upgrade.
3. From the **System State** drop-down menu, select **Deny New Service**.
4. Verify that the system displays **Denying** in the **System State** column.

Updating the Subject Alternative Name on the Manage Identity Certificate

About this task

Before starting the upgrade, update the Subject Alternative Name (SAN) on the Manage Identity Certificate for each Breeze node in the cluster. The SAN must include the node's management IP address and `127.0.0.1`, as well as the node's management FQDN.

Procedure

1. Log in to System Manager at `https://<FQDN>/SMGR/` using valid credentials.
2. Go to **Services** → **Inventory** → **Manage Elements**.
3. Select the Breeze node.
4. From **More Actions**, select **Manage Identity Certificates**.
5. Select the management service, then click **Replace**.
6. In **Replace Identity Certificates**:
   a. Select **RSA** for Key Algorithm.
   b. Select the appropriate **Key Size**. For example, **2048**
   c. Under **Subject Alternative Names**, select **DNS Name** and **IP Address**.
   d. Ensure the IP Address field contains the node's management IP and 127.0.0.1, separated by a comma:
      - If the field is empty, enter `<node management IP>,127.0.0.1`. For example, `10.92.18.231,127.0.0.1`
      - If the field already contains the node's management IP, append ,`127.0.0.1`. For example: `10.92.18.231,127.0.0.1`

e. Ensure the DNS Name field contains the node's management FQDN.

   Example: `cc118131.avaya.com`

7. Click **Commit**.
8. Repeat these steps for every remaining Breeze node in the cluster.

Verify activity

About this task

Verify that currently there is no activity on the Avaya Breeze® platform server you are upgrading.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
2. In the left navigation pane, click **Server Administration**.
3. In the row for the server you are upgrading, look in the **Activity** column.
4. Verify that the **Activity** is 0.
   - It can take a couple of hours for activity to reach zero. If activity has not stopped in a reasonable time, you can choose to proceed with the upgrade. Active calls continue but without snap-in call control.

Upgrading the Avaya Breeze® platform server

Before you begin

1. Verify that you have copied the ISO upgrade file to the server that you are upgrading.
2. Take a snapshot of the current VM to enable reverting if necessary.

Procedure

1. Log on to the Avaya Breeze® platform server.
2. Enter the command **`upgradeCE`** *<iso filename>*.
3. Step through prompts.

Upgrades using Solution Deployment Manager

System Manager Solution Deployment Manager is a centralized upgrade solution, which you can use to upgrade Avaya Breeze® platform. You can upgrade from Avaya Breeze® platform Release 3.3 or higher to the latest release.

Solution Deployment Manager accesses the OVA file in the System Manager software library.

See the following documents for more information:

- *Upgrading and Migrating Avaya Aura® applications from System Manager*
- *Administering Avaya Aura® System Manager*
- *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*

Prerequisites

- To use the Solution Deployment Manager upgrade process, you must have Avaya Breeze® platform Release 3.3 or later.
- Check you can administer the VMware host or Appliance Virtualization Platform and the Avaya Breeze® platform virtual machine in Solution Deployment Manager Application Management. For more information, see *Administering Avaya Aura® System Manager*.

Checklist for upgrading Avaya Breeze® platform using Solution Deployment Manager

This checklist outlines the process to upgrade Avaya Breeze® platform using Solution Deployment Manager.

#	Task	✔
1	Complete items 1 to 13 in "Checklist for upgrade method 2 - Simultaneous cluster upgrade" on page 53.	
2	Ensure that you install Solution Deployment Manager.	
3	Install the OVA file into the System Manager software library.	
4	Upload the `versions_edp.xml` file to Solution Deployment Manager. For more information, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.	
5	Re-establish the trust connection when upgrading applications not deployed from Solution Deployment Manager.	
6	Refresh the host status.	
7	Refresh the elements. You can either run the job schedule immediately or schedule it for a later time.	
8	Analyze the software library inventory.	
9	Perform the pre-upgrade check.	
10	Perform the upgrade using Solution Deployment Manager.	

Table continues

#	Task	✔
11	Commit the upgrade of Avaya Breeze® platform.	
12	Copy the patch file to the Avaya Breeze® platform server.	
13	Return to item 15 in "Checklist for upgrade method 2 - Simultaneous cluster upgrade" on page 53.	

Installing the Solution Deployment Manager client

Procedure

1. Download the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.zip` file from the Avaya Support website at http://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.
2. On the Avaya Support website, click **Support by Products › Downloads**, and type the product name as **System Manager**, and Release as **8.0.x**.
3. Click the **Avaya Aura® System Manager Release 8.0.x SDM Client Downloads, 8.0.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

   You can also copy the zip file to your software library directory, for example, `c:/tmp/Aura`.
4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.
5. On the Welcome page, click **Next**.
6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.
7. On the Install Location page, perform one of the following:

   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.
   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

     To restore the path of the default directory, click **Restore Default Folder**.

   The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.
8. Click **Next**.
9. On the Pre-Installation Summary page, review the information, and click **Next**.
10. On the User Input page, perform the following:

    a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.

b. To change the default directory, in Select Location of Software Library Directory, click **Choose** and select a directory.

   The default software library of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts`.

   You can save the artifacts in the specified directory.

c. In **Data Port No**, select the appropriate data port.

   The default data port is 1527. The data port range is from 1527 through 1627.

d. In **Application Port No**, select the appropriate application port.

   - The default application port is 443. If this port is already in use by any of your application on your system, then the system does not allow you to continue the installation. You must assign a different port number from the defined range. The application port range is from 443 through 543.

> **Note:**
>
> After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.

e. **(Optional)** Click **Reset All to Default**.

11. Click **Next**.
12. On the Summary and Validation page, verify the product information and the system requirements.

    - The system performs feasibility checks such as disk space and memory. If the system displays any error messages, you must make the required disk space, memory, or ports available to continue with installation.

13. Click **Install**.
14. To exit the installer, on the Install Complete page, click **Done**.

    The installer creates a shortcut on the desktop.

15. To start the client, click the Solution Deployment Manager client icon, .

Next steps

- If you are using the services port for the installation, configure the laptop to connect to the services port.
- Connect the Solution Deployment Manager client to Appliance Virtualization Platform through the customer network or services port.

  For information about "Methods to connect the Solution Deployment Manager client to Appliance Virtualization Platform", see *Using the Solution Deployment Manager client*.

Installing the OVA file into the software library

Procedure

1. Copy the previously downloaded Avaya Breeze® platform OVA file to the System Manager `/swlibrary/staging/sync/` directory.

   If necessary, add the `staging/sync` folders to the directory structure.
2. Navigate to **Home › Services › Solution Deployment Manager › Software Library Management** and click **Manage Files**.
3. In the Sync Files from directory list, enter the SHA256 checksum and select a software library.

   For **Product Family**, **Device Type**, and **Software Type**, select **others**.
4. Click **Sync** and wait for the operation to complete.
5. Verify the completion of the file sync to the library.
   a. Navigate to **Home › Services › Scheduler › Completed Jobs**.
   b. Look for Job Name = IUM_syncFiles, and Job Status = SUCCESSFUL.
6. Navigate to **Home › Services › Solution Deployment Manager › Software Library Management**.
7. To check SMGR_DEFAULT_LOCAL, click **Manage Files** and confirm that the OVA file appears in the list of files under Software Library Files.

Downloading the `version_edp.xml` file

About this task

This file provides information about your software entitlements.

Procedure

1. Log in to https://plds.avaya.com.
2. Search for the `smgr-versionsxmls.zip` using PLDS ID SMGRSUM0001:
   a. Click the **Assets** tab.
   b. Click **View Downloads**.
   c. Select **Search by Download**.
   d. In the **Download pub ID** field, enter `SMGRSUM0001`.
   e. Click **Search Downloads**.
3. Download the zip file.
4. Extract the zip file.

Re-establishing a trust connection

About this task

Use this procedure to reconnect applications not deployed from Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services › Solution Deployment Manager**.

2. In the navigation pane, click **Application Management**.
3. Select the virtual machine.
4. To establish trust, click **More actions › Re-establish connection**.
5. In the Select Version pane, select `others`.
6. Type the credentials and click **Reestablish Connection**.
    - The **Current Action Status** column displays the status of the virtual machine reestablishment.

Refreshing the host status

Procedure

1. In System Manager, click **Services › Solution Deployment Manager › Application Management**.
2. On **Application Management Tree**, click the required location.
3. Click the **Platforms** tab.

   The system displays the list of hosts for the selected location.
4. Select the required host.
5. Click **Refresh**.

   The **Current Action Status** column displays the status of the host.

Refreshing elements

About this task

Before upgrading, refresh elements on the Upgrade Management page.

Before you begin

On the User Settings page, configure the user settings.

Procedure

1. On the System Manager web console, click **Services › Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
    a. Select one or more devices.
    b. Click **Pre-upgrade Actions › Refresh Element(s)**.
4. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
5. If you selected **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays ✔ and the **Current Version** column displays the current version of the element.

Analyzing software

About this task

Analyze the OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitlement upgrade version, the **Version** field must contain the appropriate value. You can get the version values from the `version_edp.xml` file you downloaded from PLDS.

You do not need to do this process for custom patching.

Before you begin

- On the Roles page, set the Software Management Infrastructure permission.
- Refresh elements.

Procedure

1. On the System Manager web console, click **Services › Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select a device that you want to analyze.
   b. Click **Pre-upgrade Actions › Analyze**.
4. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

   The **Last Action Status** column displays a ✓, the Current Version column displays the current version of the element, and the Entitled Upgrade Version column displays the next version of the element which you can upgrade to.

Performing the pre-upgrade check

Procedure

1. On the System Manager web console, click **Services › Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
   a. Select an application to upgrade.
   b. Click **Pre-upgrade Actions › Pre-upgrade Check**.
4. On the Pre-upgrade Configuration page, fill in the required information.

   To migrate to an ESXi host from the old server, in **Target Host**, select the ESXi host.
5. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.

6. Click **Schedule**.

   On the Upgrade Management page, the status of the **Last Action Status** and **Pre-upgrade Check Status** columns display a .

Upgrading Avaya Breeze® platform using Solution Deployment Manager

About this task

Use this procedure to upgrade Avaya Breeze® platform using Solution Deployment Manager.

Before you begin

Install the Solution Deployment Manager client.

Procedure

1. Do one of the following to access Solution Deployment Manager:
   - On the System Manager web console, click **Services › Solution Deployment Manager**.
   - Navigate to **Avaya › Avaya SDM Client** from the Windows **Start** menu.
   - Click the Solution Deployment Manager client icon () on your desktop.
2. In the navigation pane, click **Upgrade Management**.
3. Click the Avaya Breeze® platform application to upgrade.
4. Click **Upgrade Actions › Upgrade/Update**.
5. On the Upgrade Configuration page, to view the devices associated with the application that you want to upgrade, do the following:
   a. Click **Details** and review the dependent devices.
   b. Click **Done**.
6. To continue with upgrade when the recommended checks fail during the pre-upgrade check, select the **Override pre-upgrade check** checkbox.
7. To provide the upgrade configuration details, click **Edit**.
8. To upgrade:
   a. Select the appropriate ESXi host.
   b. In the **Upgrade Source** field, select **SMGR_DEFAULT_LOCAL**.
   c. In the **Upgrade To** field, select the OVA file.
   d. In **Existing Administrative User**, type the customer login name.
   e. In **Existing Administrative Password**, type the customer login password.
   f. Click **Pre-populate Data**.

      The system populates the data for the following fields:

      - **IP Address**
      - **Short Hostname**
      - **Network Domain**
      - **Netmask**
      - **Default Gateway**
      - **DNS server(s)**

- **Timezone**
- **NTP server(s)**
- **Login Name**
- **Enter Customer Account Password**
- **Primary System Manager IP**
- **Enrollment Password**
- **Accept the License Agreement**

g. In the **Flexi Footprint** field, select the footprint based on the user requirement.

h. Do one of the following in the **EASG User Access** field:

- Type 1 to enable EASG.

  Avaya recommends that you enable EASG.
- Type 2 to disable EASG.

i. In the **Public** field, select the network that will support the Avaya Breeze® platform security module network.

j. In the **Out of Band Management** field, select the network that supports the Avaya Breeze® platform management network.

k. In the **Datastore** field, select the datastore that supports the Avaya Breeze® platform server.

l. Click **Save**.

9. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

   If the field displays , review the information on the Edit Upgrade Configuration page.

10. On the Upgrade Configuration page, click **Upgrade**.
11. On the Job Schedule page, click one of the following:

    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.

12. Click **Schedule**.
13. Click **Upgrade**.
14. To view the upgrade status, do the following:

    a. In the navigation pane, click **Upgrade Job Status**.

    b. In the **Job Type** field, click **Upgrade**.

    c. Click the upgrade job that you want to view.

15. Verify that the upgrade of the application is successful.

Committing the upgrade of Avaya Breeze® platform

Procedure

1. In System Manager, click **Services › Solution Deployment Manager › Upgrade Management**.

2. Select the Avaya Breeze® platform by selecting the check box to the left of the **Name** column.
3. In the **Upgrade Actions** menu, click **Commit/Rollback Upgrade**.

   The system displays the Job Schedule page.
4. Select **Commit** in the **Upgrade Actions** column.
5. Click **Run Immediately** to perform the job now or click **Schedule later** to perform the job at a scheduled time.
6. Click **Schedule**.

   The system returns to the Upgrade Management page.
7. Click **Enable Auto Refresh**.

   The system updates the **Last Action** and **Last Action Status** fields when the Commit job is complete.
8. Click the icon in the **Last Action Status** field.

   The system displays the Element Check Status dialog box.
9. Click **Done**.
10. To view the Commit job status, perform the following:
    a. In the navigation pane, click **Upgrade Jobs Status**.

       The system displays the Upgrade Jobs Status page.
    b. In the **Job Type** menu, click **Commit/Rollback Upgrade**.
    c. In the **Job Name** column, click the job that you want to view.
    d. Click **Done**.

Verifying replication status

About this task

Complete this task to verify that the System Manager database replicated to Avaya Breeze® platform.

Procedure

1. In System Manager, click **Services › Replication**.
2. Locate the Avaya Breeze® platform in the **Replica Group** list.
3. In the **Synchronization Status** column, verify that the Avaya Breeze® platform status is `Synchronized`.

   - Depending on the amount of data, the replication might take some time to complete. Refresh the page or periodically recheck the status.
   - If the status is not `Synchronized`, for more information, see *Maintaining and Troubleshooting Avaya Breeze® platform*.

Running maintenance tests

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.

2. In the navigation pane, click **System Tools And Monitoring › Maintenance Tests**.
3. In the **Select Avaya Breeze® to test** field, select an Avaya Breeze® platform server from the drop-down menu.
4. To run all the tests, click **Execute All Tests**.
5. To run specific tests:
   a. Select the test or tests that you want to run.
   b. Click **Execute Selected Tests**.

Verifying server status

About this task

Verify that the Avaya Breeze® platform server has upgraded to Release 3.9 and is functioning correctly.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
2. In the row for the server you are upgrading, verify the following information:
   - The **Service Install Status** is a green checkmark
   - The **Security Module** is Up
   - The **License mode** is a green checkmark
   - The **Version** displays release 3.1.1.

Accepting new service

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
2. Select the server and click **System State › Accept New Service**.
3. Verify that the **System State** column for the server changes to **Accepting**.

Verifying the Entity Link connection

About this task

Use this procedure to verify that Session Manager can connect with Avaya Breeze® platform using the SIP entity link. You must verify the status of SIP link monitoring on the Session Manager instance.

Procedure

1. In System Manager, click **Elements › Session Manager › System Status › SIP Entity Monitoring**.
2. Click the name of the Session Manager instance that you linked to Avaya Breeze® platform.

   The system displays a list with the status of all entity links for the selected Session Manager.
3. Locate the Avaya Breeze® platform SIP entity and check **Conn. Status**.

If you see UP, the link to Session Manager is successful. Otherwise, use the troubleshooting information in *Maintaining and Troubleshooting Avaya Breeze® platform*.

Installing new snap-ins

About this task

Complete this procedure to install new snap-ins on the upgraded cluster and to optionally install new versions of updated snap-ins. Be sure to install the newest versions of connector snap-ins and the snap-ins that are mandatory for your cluster profile. Mandatory services for a cluster profile listed on the Cluster Editor page. For a list of connector snap-ins, see *Avaya Breeze® platform Overview and Specification*.

Procedure

1. In System Manager, click **Elements › Avaya Breeze® › Service Management**.
2. Load the snap-in.
   a. Click **Load**.
   b. In the Load Service window, click **Choose file**, browse to select your snap-in and click **Open**.
   c. Click **Load** in the Load Service window.
   d. For licensed snap-ins, if you agree to the Avaya End User License Agreement (EULA), click **Accept**.

      Your snap-in displays on the Service Management page with a **State** of **Loaded**.
3. Install the snap-in.
   a. Select the snap-in you want to install.
   b. Click **Install**.
   c. Select the clusters where you want the snap-in to reside and click **Commit**.
   d. To see the status of the snap-in installation, click the **Refresh Table** icon located in the upper-left corner of the **All Services** list.

      Installed with a green check mark indicates that the snap-in has completed installation on all servers in the cluster. **Installing** with a yellow exclamation mark enclosed in a triangle indicates that the snap-in has not completed installation on all servers.

Setting preferred snap-in version

About this task

It is possible to set a preferred version of a snap-in. A service profile uses this to indicate the version of the snap-in to provide to a group of users. You must first designate the version of the snap-in that is the preferred version. Then, change the version designation for the snap-in in the service profile. For more information about service profiles and version designations, see *Administering Avaya Breeze® platform*.

Non-call-intercept snap-ins automatically use the preferred version if specified, otherwise they use the latest version. Service profiles do not include non-call-intercept snap-ins.

Procedure

1. Designate the preferred version:
   a. On System Manager, click **Elements › Avaya Breeze® › Service Management**.
   b. From the **All Services** list, select the version of the snap-in that you want to be the preferred version.
   c. Click **Set Preferred Version**.
   d. Select the clusters for which you want this to be the preferred version and click **Commit**.

   Note:

   - You can set the preferred version for multiple snap-ins in a single transaction.

2. Edit the service profile:
   a. On System Manager, click **Elements › Avaya Breeze® › Configuration › Service Profiles**.
   b. Select the service profile and click **Edit**.
   c. Remove the snap-in from the service profile by clicking the **X** next to the snap-in name.
   d. In the list of **Available Service to Add to this Service Profile** click **Advanced** next to the snap-in name.
   e. For **Service Version** select **Preferred** and click **Add**.
   f. Click **Commit** to save the service profile.

Chapter 7: Enhanced Access Security Gateway

Avaya Breeze® platform supports Enhanced Access Security Gateway (EASG). EASG is a certificate-based, challenge-response authentication and authorization solution.

EASG provides a secure method for Avaya services personnel to:

- Access Avaya Breeze® platform remotely and onsite. As the customer, you can enable or disable access at any time.
- Perform tasks necessary for the ongoing support, management, and optimization of the solution.
- Enable remote proactive support tools such as Avaya Expert Systems® and Avaya HealthCheck.
- Perform the required maintenance tasks.

EASG only supports Avaya services logins, such as init, inads, and craft.

Enabling and disabling EASG

About this task

By enabling Avaya Services logins, you are granting Avaya access to your system. This allows Avaya to resolve product issues in a timely manner.

Before you begin

- You must registered the product using the Avaya Global Registration Tool (GRT) at https://grt.avaya.com. See https://support.avaya.com/registration for additional information on registering products for remote access and alarming.

Procedure

1. Log in to the Avaya Breeze® platform CLI interface using your customer account.
2. To check the status of EASG, run the command: `EASGStatus`.
3. To enable EASG, run the command: `EASGManage –-enableEASG`.
4. To disable EASG, run the command: `EASGManage –-disableEASG`.

Viewing the EASG certificate information

About this task

Use this procedure to view information about the product certificate, which includes information about when the certificate expires.

Procedure

1. Log in to the Avaya Breeze® platform CLI interface using customer account.
2. Run the following command: `EASGProductCert --certInfo`.

EASG site certificate

Onsite Avaya technicians use the EASG site certificates to respond to EASG challenges when accessing a server. The technician generates and provides the EASG site certificate to the customer. The customer loads the EASG site certificate onto each Avaya Breeze® platform server to which they want to grant the technician access.

The EASG site certificate only allows access for the Avaya technician. Other users, including other Avaya technicians cannot use it. After the technician completes their work, the customer can remove the EASG site certificate from the server or it is automatically removed by the EASG software when the site certificate expires.

Managing site certificates

Before you begin

Obtain the site certificate from the Avaya support technician and install it to Avaya Breeze® platform. Note the location of this file and use it in place of *installed_pkcs7_name* in the following commands.

Procedure

1. Log in to the Avaya Breeze® platform CLI interface using customer account.
2. To install the site certificate:
   a. Run the following command: `EASGSiteCertManage –add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.
3. To view information about a particular certificate: run the following command:
   - To list the site certificates installed on the system: `EASGSiteCertManage --list`
   - To display detailed information about a specified site certificate: `EASGSiteCertManage --show <installed_pkcs7_name>`
4. To delete the site certificate, run the following command:
   - To delete the specified site certificate: `EASGSiteCertManage --delete <installed_pkcs7_name>`
   - To delete all site certificates installed on the system: `EASGSiteCertManage --delete all`

Chapter 8: Patching

This section of documentation covers the process and considerations for patching Avaya Breeze® platform.

Determining patching sequence

About this task

If you do not have snap-ins that use the cluster database, patch the servers in any sequence one at a time. See "Patching the Avaya Breeze platform" on page 97. If you have multiple servers in a cluster and have snap-ins that use the cluster database, you must patch the servers in the correct sequence to avoid customer impact. The sequence depends on the active, standby, or idle status of the server. Follow the sequence in this procedure to patch your servers.

Procedure

1. In System Manager, click **Elements › Avaya Breeze®**.
2. In the navigation pane, click **Cluster Administration**.
3. Click **Show** in front of the cluster you are patching to see the servers in the cluster.
4. In the Cluster Database column, identify the Active, Standby and idle servers.
5. Patch all idle servers one at a time.
6. Patch the server with the Standby cluster database.
7. Switch the active server to standby by clicking on **Active** in the **Cluster Database** column.
8. Click **Continue** to complete the switch to Standby.
9. Patch the server that now is the Standby.

Patching the Avaya Breeze® platform

About this task

This procedure provides general patching steps. For more information about specific patches, see *Avaya Breeze® platform Release Notes*.

⚠ Caution:

You cannot remove a patch after it is installed. This includes recovery from a patch install failing due to intermittent network issues. To enable recovery, you must take a snapshot of Avaya Breeze® platform before installing the patch. Verify that the system is running correctly after the patch is installed. When verified, remove the snapshot within 12–24 hours. See "VMware snapshots" on page 99 for special considerations when using snapshots.

Before you begin

- The server must be in the Deny New Service state.
- Ensure that the activity count is 0 for a cluster database.
- Download the patch file and copy it to the Avaya Breeze® platform server.
- The patch should have the following Linux permissions: `rw-r--r--`.

Procedure

1. Log in to Avaya Breeze® platform using the customer account.
2. Execute the `patchCE` command.

   For example: `$ patchCE –i /home/cust/<patchname>.bin`
3. When prompted that the patch is service interrupting, answer **Yes** and press `Enter`.

   The patch installs. Wait for the patch installation to complete. Depending on the patch, Avaya Breeze® platform may reboot.
4. Verify the version of the installed patch. The version can be viewed in one of the following ways:
   - Log in to Avaya Breeze® platform and execute the command `patchCE –s`.
   - Log in to Avaya Breeze® platform and execute the command `swversion`.
   - On System Manager, click **Elements › Avaya Breeze® › Server Administration**.
5. In System Manager, click **Elements › Avaya Breeze® › Server Administration**.
6. Identify the row for the Avaya Breeze® platform server you are patching and verify the following:
   - The **Service Install Status** is a green checkmark.
   - The **Security Module** is Up.
   - The **License mode** is a green checkmark.
   - The **Version** displays the new release.

Patch command options

The patch command takes the form **`patchCE [action] [patch file]`** where:

- **`[action]`** is one of the following. If not included, the assumed action is to install the specified patch file.
  - **`i`** = Install the patch file.
  - **`s`** = Show patch information for binary or installed patch.
  - **`v`** = Verify that the server can install the patch file.
- **`[patch file]`** is the full path to the patch file including the file name.

Appendix A: VMware snapshots

A snapshot preserves the state and data of a virtual machine at a specific point in time. You can create a snapshot before upgrading or installing a patch.

The best time to take a snapshot is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

⚠ Caution:

Snapshot operations can adversely affect service. Before performing a snapshot operation, you must stop the application that is running on the virtual machine or place the application out-of-service. When the snapshot operation is complete, start or bring the application back into service.

Only take snapshots during a maintenance window.

Snapshots can:

- Consume large amounts of data resources.
- Increase CPU loads on the host.
- Affect performance.
- Affect service.

To prevent adverse behaviors, consider the following recommendations when using the Snapshot feature:

- Do not rely on VMware snapshots as a robust backup and recovery method. Snapshots are not backups. The snapshot file is only a change log of the original virtual disk.
- Do not run a virtual machine from a snapshot. Do not use a single snapshot for more than 24 to 72 hours.

  If your virtual machine contains snapshots that are more than 72 hours old, system performance might be impacted. When you no longer need a snapshot, remember to delete it.
- Take the snapshot, make the changes to the virtual machine, and delete or commit the snapshot after you verify the virtual machine is working properly. These actions prevent snapshots from growing so large as to cause issues when deleting or committing the snapshots to the original virtual machine disks.
- When taking a snapshot, do not save the memory of the virtual machine. The time that the host takes to write the memory to the disk is relative to the amount of memory that the virtual machine is configured to use. Saving the memory can add several minutes to the time taken to complete the operation. If the snapshot is active, saving memory can make calls appear to be active or in progress and can cause confusion to the user. To

create a clean snapshot image from which to boot, do the following when you create a snapshot:

  - In the Take Snapshot window, clear the **Include virtual machine's memory** check box.
  - Select the **Quiesce guest file system (Needs VMware Tools installed)** check box to ensure that all write instructions to the disks are complete. You have a better chance of creating a clean snapshot image from which to boot.

- If you are going to use snapshots for a long time, you must consolidate the snapshot files regularly to improve performance and reduce disk usage. Before merging the snapshot delta disks back into the base disk of the virtual machine, you must first delete stored snapshots.

  Note:

  If a consolidation failure occurs, end-users can use the actual Consolidate option without opening a service request with VMware. If a commit or delete operation does not merge the snapshot deltas into the base disk of the virtual machine, the system displays a warning on the user interface.

Related resources

Title	Link
Best practices for virtual machine snapshots in the VMware environment	Best Practices for virtual machine snapshots in the VMware environment
Understanding virtual machine snapshots in VMware ESXi and ESX	Understanding virtual machine snapshots in VMware ESXi and ESX
Working with snapshots	Working with snapshots
Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots	Send alarms when virtual machines are running from snapshots

Appendix B: Removing obsolete Avaya Aura Media Server configuration

Removing obsolete Avaya Aura® Media Server configuration

This section covers the processes for removing obsolete Avaya Aura® Media Server configuration instances.

Checklist for removing obsolete Avaya Aura® Media Server configuration in System Manager

No.	Task	Reference	✔
1	Remove the Avaya Aura® Media Server routing pattern.	See "Removing the Avaya Aura Media Server routing pattern" on page 101	
2	Remove the SIP entity links for Avaya Aura® Media Server.	See "Removing SIP entity links for Avaya Aura Media Server" on page 102	
3	Remove the SIP entities for each Avaya Aura® Media Server.	See "Removing the SIP entity for each Avaya Aura Media Server" on page 102	
4	Remove the Avaya Aura® Media Server host name resolution.	See "Removing the Avaya Aura Media Server host name resolution" on page 102	

Removing the Avaya Aura® Media Server routing pattern

Procedure

1. In System Manager, click **Elements › Routing › Routing Policies**.
2. Select the routing pattern created for Avaya Aura® Media Server.
3. Click **Delete**.
4. In the navigation pane, click **Regular Expressions**.
5. Select the regular expression created for Avaya Aura® Media Server.
6. Click **Delete**.

Removing SIP entity links for Avaya Aura® Media Server

Procedure

1. In System Manager, click **Elements › Routing › Entity Links**.
2. Select the entity link created for Avaya Aura® Media Server.
3. Click **Delete**.

Removing the SIP entity for each Avaya Aura® Media Server

Procedure

1. In System Manager, click **Elements › Routing › SIP Entities**.
2. Select the SIP entity created for each Avaya Aura® Media Server.
3. Click **Delete**.

Removing the Avaya Aura® Media Server host name resolution

Procedure

1. In System Manager, click **Elements › Session Manager › Network Configuration › Local Host Name Resolution**.
2. Select the FQDN host name created for Avaya Aura® Media Server.
3. Click **Delete**.

Appendix C: Documentation for Collaboration Environment

Additional information

The following resources provide additional information.

Documentation

See the following related documents at https://support.avaya.com. Many documents are also available at https://documentation.avaya.com.

Overview

Title	Use this document to:	Audience
Avaya Breeze® platform Overview and Specification	Understand the Avaya Breeze® platform, customer requirements, and design considerations.	Sales engineers Programmers System administrators Services and support personnel
Avaya Aura® System Manager Overview and Specification	Understand System Manager customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel

Table continues

Title	Use this document to:	Audience
Avaya Aura® Media Server Overview and Specification	Understand Avaya Aura® Media Server customer requirements and design considerations.	Sales engineers Programmers System administrators Services and support personnel

Deploying

Title	Use this document to:	Audience
Deploying Avaya Breeze® platform	Deploy and configure Avaya Breeze® platform. This is the main deployment document for Avaya Breeze® platform. The deployment documents for other environments are listed below.	Implementation engineers Support personnel System administrators
Deploying Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform	Deploy Avaya OneCloud™ CPaaS-enabled Avaya Breeze® platform.	Implementation engineers Support personnel System administrators
Quick Start to deploying the HelloWorld Snap-in	Install, configure, and test an Avaya Breeze® platform snap-in service, specifically the HelloWorld call intercept snap-in.	Programmers System administrators
Planning for Deploying Avaya Aura® applications	Understand deployment options for various Avaya Aura® applications.	Services and support personnel System administrators

Table continues

Title	Use this document to:	Audience
Deploying and Updating Avaya Aura® Media Server Appliance	Deploy and configure Avaya Aura® Media Server when it is installed on customer-provided servers.	System administrators Services and support personnel
Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment	Deploy and configure Avaya Aura® System Manager in an IaaS environment. A separate document is also available for deploying System Manager in a virtualized environment.	System administrators Services and support personnel

Administering

Title	Use this document to:	Audience
Administering Avaya Breeze® platform	Administer Avaya Breeze® platform and snap-ins.	System Administrators Services and Support personnel
Implementing and Administering Avaya Aura® Media Server	Deploy and configure Avaya Aura® Media Server.	System administrators Services and support personnel
Administering Avaya Aura® System Manager	Administer Avaya Aura® System Manager.	System Administrators Services and support personnel
Administering Avaya Aura® Session Manager	Administer Avaya Aura® Session Manager.	System Administrators Services and support personnel

Table continues

Title	Use this document to:	Audience
Administering Avaya Session Border Controller	Administer Avaya SBC.	System Administrators Services and support personnel

Maintaining and troubleshooting

Title	Use this document to:	Audience
Upgrading Avaya Breeze® platform	Upgrade Avaya Breeze® platform.	Services and support personnel
Maintaining and Troubleshooting Avaya Breeze® platform	Troubleshoot Avaya Breeze® platform.	Services and support personnel System administrators
Troubleshooting Avaya Aura® System Manager	Troubleshoot System Manager.	Services and support personnel
Troubleshooting Avaya Aura® Session Manager	Troubleshoot Avaya Aura® Session Manager.	Services and support personnel

Programming

The following developer documents are available on Avaya DevConnect .

Title	Use this document to:	Audience
Getting Started with the Avaya Breeze® platform SDK	Deploy and configure the Eclipse IDE, Apache Maven, and the Avaya Breeze® platform SDK.	Programmers
Avaya Breeze® platform Snap-in Development Guide	Understand the key concepts needed to develop the different types of Avaya Breeze® platform snap-ins.	Programmers

Table continues

Title	Use this document to:	Audience
Avaya Breeze® platform FAQ and Troubleshooting for Snap-in Developers	Troubleshoot Avaya Breeze® platform snap-in developer issues.	Programmers
Avaya Breeze® platform API Javadocs	Understand API classes and uses.	Programmers

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support › Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.

- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at https://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field, and click **Go** to search for the course.

Course code	Course title
43750W	Selling Avaya Custom and Integration Solutions
30210W	Avaya Breeze® platform Overview for Design
30810W	Designing the Avaya Breeze® Solution Part 1 of 2
30820W	Designing the Avaya Breeze® Solution Part 2 of 2
39220W	Avaya Breeze® Release 3.8 Details for Pre-Sales
39240W	Avaya Breeze® UC Snap-ins Release 3.8 Details for Pre-Sales
2016W	Avaya Breeze® platform Fundamentals
20240W	Programming Avaya Breeze® platform Snap-ins Using Java SDK
20250W	Creating Avaya Breeze® platform Workflows Using Engagement Designer
20260W	Creating Advanced Avaya Breeze® platform Workflows Using Engagement Designer
7016W	Avaya Breeze® platform Implementation and Support
71300V	Integrating Avaya Aura® Communication Applications
72300V	Supporting Avaya Aura® Communication Applications

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Developer resources

Avaya DevConnect provides resources for Avaya Breeze® platform developers. You must register to access the DevConnect website.

Basic DevConnect membership is free and gives you access to the following information and resources:

- Programming and product documentation
- Sample applications
- Videos
- Webinar recordings
- Forums

Upgraded membership options offer developer-oriented technical support and other program services.

Use a browser to navigate to the Avaya Breeze® platform DevConnect website at https://www.avaya.com/breezedeveloper.

Support

Platform support

Go to the Avaya Support website at https://support.avaya.com/ for the most up-to-date documentation and product notices. You can also search for release notes, service packs, and patches. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Product documentation is also available on the Avaya Documentation Center at https://documentation.avaya.com.

Developer support

Go to the Avaya DevConnect website at http://www.avaya.com/breezedeveloper to access the Avaya Breeze® platform API, SDK, sample applications, developer-oriented technical documentation, and training materials.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support › Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Index

Special Characters

_REPLACE THIS TEXT, OR DELETE THIS ENTIRE INDEXTERM ELEMENT IF YOU DO NOT NEED IT 30, 60

A

AAMS support 10
accepting new service 71, 51, 92
active cluster database server
  identifying 79
  upgrade sequence 78
adding Avaya Breeze server 47
adding nodes 47
analyze inventory
  SDM 67
analyzing software 67
applications
  pre-upgrade check 67
assigning
  media server 27
automatic restart
  virtual machine 42, 43, 42
Avaya Aura Media Server selection algorithm ... 11
Avaya InSite Knowledge Base 111

C

certificate enrollment password 30
changes 8
checklist
  method 3 74
  obsolete Avaya Aura Media Server configuration 101
  rolling cluster upgrade 74
  SDM 62
cluster
  accepting new service 51
  attributes 47
  denying service 31
  reboot 50
  restore 50
  verify activity 31
cluster database servers
  identifying 97
cluster IP 47
collection
  delete 107
  edit 107
  generating PDF 107
  sharing content 107
committing upgrade 69
Communication Manager support 10
configuring
  VM automatic restart 42, 43, 42
content
  publishing PDF output 107
  searching 107
  sharing 107
  sort by last updated 107
  watching for updates 107
craft account 8
Creating multiple privileged user accounts 44
customer account 8
customer configuration information
  ISO requirements 58, 78
  locating 21
customer password 44

D

deleting host name 102
deleting routing pattern
  Media Server 101
deleting SIP entity
  Media Server 102
deleting SIP entity links
  Media Server 102
deny service 60, 31, 81
deploy
  upgrade OVA 34
deploying using SDM 40
deploying using vSphere client 34
Deploying using web-based client 35
DevConnect 110
document changes 8
documentation center 107
documentation center
  finding content 107
  navigation 107
documentation portal 107
downloading software 58, 79

E

EASG 95
EASG
  certificate information 95
  disabling 95
  enabling 95
  site certificates 96
EASG site certificate 96
elements
  refresh 66

Enhanced Access Security Gateway 95
Enrollment Password status 59, 80
enrollment password status 30
entitlement analysis 67
entity link
verification 71, 51, 92
entity links
removing 102
ESXI
upgrade 11

F

finding content on documentation center 107

G

GDPR 14

H

host name resolution
Avaya Aura Media Server 102
removing Media Server configuration 102
HTTP traffic 47

I

idle cluster database server
identifying 79
upgrade sequence 78
install
trust certificates 50
installing OVA
into software library 65
inventory
refresh elements 66
ISO upgrade 74, 53
ISO upgrade
simultaneous cluster upgrade 53

K

KB
Support site 111

L

licensing upgrades 11
load balancing 47

M

maintenance
VMware 11
maintenance tests
on-demand 70, 48, 91
memory reservation 16
memory reservation
increasing 16
method 1 16
method 2 53
multiple user accounts
configure 44
create 44

O

OVA
deploy 34
OVA deployment
vSphere client connected to ESXi host 37
with SDM 40
with vCenter 34
with VMware vSphere web client 35
OVA to software library 65
OVA upgrade 16
OVA upgrade
simultaneous cluster upgrade 53

P

patch command options 98
patching 97
patching the server 97
permissions 10, 8
PLDS 53, 11, 16
PLDS
downloading software 58, 29, 79
pre-upgrade check
applications 67
Pre-upgrade Configuration 67
preferred version 72, 45, 93
prepare for an upgrade 10

R

refresh elements in inventory 66
refreshing host 66
removing Avaya Breeze server 32
removing FQDN host name 102
removing nodes 32
removing obsolete Avaya Aura Media Server configuration 101
removing routing pattern
Media Server 101
removing SIP entity
Media Server
Avaya Aura Media Server 102
removing SIP entity links
Avaya Aura Media Server 102
Media Server 102
removing the Avaya Aura Media Server routing pattern 101
replication status verification 70, 48, 91
REST 26
restore 50
routing pattern
removing 101

S

SDM OVA deployment 40
searching for content 107
secure grid
  disabling 29, 59, 80
  enabling 47
security
  trust certificates 50
server
  accepting new service 71, 92
  denying service 60, 81
  iso file upgrade command 61, 82
  verify activity 61, 82
servers
  shutdown 33
service impact 16
service profiles 72, 45, 93
services
  uninstall 32
Session Manager support 10
sharing content 107
shut down servers 33
simultaneous cluster upgrade 53
SIP entity
  removing 102
SMGR_DEFAULT_LOCAL 65
snap-ins
  installing new 72, 49, 93
snapshots 99
Solution Deployment Manager 61, 67
Solution Deployment Manager client 63
Solution Deployment Manager upgrade checklist .. 62
sort documents 107
standby cluster database server
  identifying 79
  upgrade sequence 78
status
  Enrollment Password 59, 80
  enrollment password 30
  server 71, 48, 92
support 110
System Manager compatibility 10
System Manager license upgrade 11
System Manager support 10

T

training 108
trust certificates 50
trust connection 65

U

uninstall
  services 32
uninstalling a service 32
upgrade
  ESXI 11
  OVA 16
  SDM 68
upgrade checklist 53, 53, 16
upgrade command 61, 82
upgrade preparation 10
upgrade requirements 10
upgrade sequence with ISO upgrades 78
upgrade status check 71, 48, 92
upgradeSolution script
  System Manager 10
upgrading 13
upgrading
  ISO upgrade 53
  simultaneous cluster upgrade 53
  upgrade paths 13

V

verification
  entity link 71, 51, 92
  replication status 70, 48, 91
  server upgrade status 71, 48, 92
verify activity 61, 82
version_edp.xml file
  downloading 65
videos 109
virtual machine
  automatic restart 42, 43, 42
VMware
  upgrade 11
vSphere client connected to ESXi host 37
vSphere client OVA deployment 34
vSphere web client OVA deployment 35

W

watchlist 107